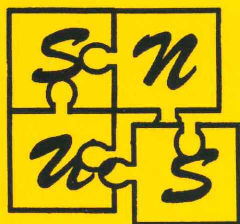


Swedish Network Users Society

1996

96 INTEROPERABILITET TESTRAPPORT

Brandvägg/Firewall

Elektronisk post/E-mail

ATM LANemulering/emulation

IT-COUNTRY

Internetdagen

DELTAGARE

• 3Com Nordic • AU- SYSTEM • Bay Networks Nordic • Cisco Systems • Combitech Nexus • DES Communications • Digital Equipment • Exo Data • GE Info Services • Global One/France Telecom • Media Communications • Microsoft • Netgain • Network Management • Salcom • Signum Support • Sun Microsystems • TeamWARE • Telia • Tele2 • UB Networks • Verimation m fl

• Datateknik/Mässtidning • Computer Sweden • Nätverk & Kommunikation • Nätvärlden

SNUS Interoperabilitet-96 stöds av Interop Company, USA

Tanken med IT-Country var att visa på framtiden redan idag. Vi kan nu visa hur Sverige bör bygga upp sin Internetstruktur för att klara en exponentiell ökning av trafik och användare i Sverige. Detta kan lösas genom att placera flera neutrala hopkopplingspunkter i Sverige. På så sätt får man ett mer finmaskigt nät och trafiken behöver inte transporteras lika långt som tidigare. Vidare kan företag ansluta sig till två operatörer för att få lastdelning och backup, för att skydda sig mot avbrott.

Testrapporten

Vi har på följande sidor gjort en sammanfattning av testerna som en introduktion. Testrapporterna finns i sin helhet i avsnitt 3-5. Leverantörerna fick innan rapporten gick i tryck möjlighet att kommentera innehållet. Testrapporterna har successivt som "draft" gjorts tillgängliga på elektroniskt media sedan 20 april 1996 .
De godkända testrapporterna finns också på SNUS www-sida under path;

http://www.snus.se

SNUS vill genom att distribuera dessa testrapporter öka kunskapen om vad som fungerade vid interoperabilitetstesterna. Detta därför att man skall kunna göra system och produktval så att konurrenskraften och effektiviteten stärks inom svensk industri och organisationer .

Tack

Årets Interoperabilitet har lyft ambitionen till att även testa funktioner i ett land i miniatyr. Det har varit en stor utmaning som deltagarna i SNUS klarat med mycket gott betyg. Detta har inte minst uppmärksammats från fackpress, radio, utställare och deltagare. Jag vill rikta ett speciellt tack till alla testledare och personer som arbetar inom SNUS och speciellt till: Patrik Fältström, Lars-Johan Liman, Peter Löthberg, Niklas Gerdin, Staffan Hagnell, Per Eriksson, Lars Beijar, Mikael Olsson, Monica Buschebane, Björn Larsson, Assar Westerlund, Jan Michael Rynning, Robert Malmgren, Pär Ahrén, Tomas Törnblom, Anders Sandell mfl.

Stockholm 7 juli 1996
Östen Frånberg

Ordförande SNUS

SNUS har som mål att för användarna:

- driva på utvecklingen av datanät och samtrafik.
- anordna seminarier och tester
- utbyta information och erfarenheter.
- teckna avtal med operatörer (drift)

1. Introduction

Interoperability = Cooperation

For the fifth year in a row, Swedish Network Users Society (SNUS) has completed its annual test program in the field of interoperability. This year we choose to work with the most important and urgent issues in order to increase the construction and development of networks and network supported services in Sweden. Our concept was to augment cooperation between suppliers and their different products, in accordance with the open standard that already has been implemented. We also furnished the suppliers with an opportunity to show their capacity to partake in big-scale comprehensive tests.

Interoperability -96 consisted in **Product Testing**, **IT-Country**, **Seminars**, and **The Internet Day**. In the Product Testing program we focused on issues regarding Firewall, mail, and LAN-emulation during a period that stretched from January, through April 1996. The results was presented during the Interoperability Days (May 8-May 10). IT-Country was a concept originally launched by Peter Löthberg, (STUPI) and involved tests on a more functional level (services), where a miniature scale-model of an "IT-Sweden" was used.

The seminars were focusing on two different themes: Technology and Management. A thematic introduction was held everyday by key-note speakers (cf. paragraph 6, in the seminar schedule).

The third day of the Interoperability Days was dedicated to The Internet Day, where results from Product Testing, as well as experiences gained from the IT-Country project was presented, i.e. in the form of "guided tours" to the benefit of the audience. Different relevant and important areas of technology was presented in a pedagogical fashion during The Internet Day.

During the Interoperability Days our goal was to present what actually works in practice. The participants had the possibility to take part in the opportunities of technology, and to scrutinize how these opportunities were implemented by the suppliers. The point was here to help create better conditions for the development of networks in a "home environment", leading to the augmentation of competitive standards in Swedish business and industry, due to a state of the art infra structure.

Interoperability -96

This year's Interoperability Days was preceded by a whole year of thorough and intense planning in order to prepare for the testing scheme, and to select relevant seminar programs. During the Interoperability Days -96 we carried out four testing programs, and 29 seminars. A large group of highly recognized persons from the supplier side, and from universities and academies, was present at the Interoperability Days. One of the concepts was to arrange so that the audience could take part of a specific problem in theory, and then see how it could be implemented in practice. The Interoperability Days was extensively covered by the media (cf. chapter 6).

Test reports

The testing scheme at the Interoperability Days involved Product Testing, Firewall, mail, ATM-LAN-emulation, IT-Country, and The Internet Day. In the following pages we have made a summary that serves an introductionary purpose, while the full test reports are to be found in section 3-6.

The suppliers have been consulted before publishing, and the test reports have been completed by their own comments and additions regarding further adaptations of their products.

The reports can also be found on SNUS's Homepage at **http://www.snus.se**

By publishing the test reports SNUS hopes to increase knowledge in the field of interoperability in order to make it easier for the client to chose between different system solutions, as well as products. The final aim is to strengthen the competitiveness and efficiency among corporations and public organizations in Sweden.

Acknowledgments

During the Interoperability Days we lifted our ambitions to a new and higher level by operating with a miniature scale model of an entire country. This was a great challenge for all the participants, and was realized in the most extraordinary way, which also stirred a lot of attention in the media. We would therefore like to thank all the test operators, as well as the staff of SNUS; and in particular Patrik Fältström, Lars-Johan Liman, Peter Löthberg, Niklas Gerdin, Staffan Hagnell, Per Eriksson, Lars Beijar, Mikael Olsson, Monica Bouchebane, Björn Larsson, Assar Westerlund, Jan-Mikael Rynning, Robert Malmgren, Per Ahrén, Tomas Törnblom, Anders Sandell etc.

Stockholm, July 7, 1996

Östen Frånberg, Chairman, SNUS
Swedish Network User's Society.

Our goals are to

- increase the development of networking and network supported communications,
- organize seminars and tests,
- take part in the exchange of information and ideas,
- sign contracts with operators.

2. Summary of testreports

FIREWALL
The manufactures and distributors configured their products and also participated in the four testteams which performed the tests.

An organization wants to protect it's internal network (intranet) by designing a protection based on the application gateways (proxys), IP-, and filterfunctions etc. The combination of these functions is called firewalls.

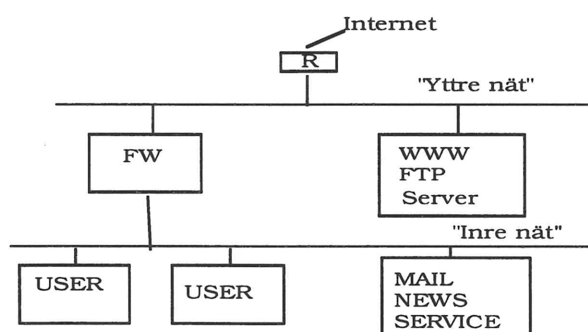
Security on the Internet has become an increasingly important issue. There are several methods and products that could be used to protect users, sessions and data. The interest of firewalls has increased during the past months, and several consultants perform tests and configurations today. SNUS has therefore developed a testspecification and performed tests on eight separate configurations of the most popular firewall-products of today.

The general testconditions were such that the firewall should protect users from attacks at the same time as letting normal traffic for www, gopher, FTP, Telnet, Ping, First class and Real Audio pass.

There were two types of test performed; positive and negative tests. Positive tests means that the correct traffic has passed. Negative tests means that users can not penetrate the firewalls.

Tested services:
* www
* gopher
* FTP
* Telnet
* Ping
* First Class
* Real Audio

Tested products:
* Pix
* BorderWare Firewall 3.1.1
* TIS Gauntlet 3.1
* TIS Gauntlet 3.1
* TIS Gauntlet 3.1
* Firewall 1, 2.0 c
* Firewall 1, 2.0
* Digital Firewall 2.0



The general results of the tests are:

- All firewalls resist all attacks made from specialized cracking tools such as ISS and Satan. We found a number of weak spots when testing the firewalls. Among them the most important were:

- The computer and the operating system are easier to penetrate than the firewall itself.

- The firewall can be flooded by a cracker sending to much traffic for it. That can lead to a breakdown of the firewall.

- The test result can be found in the reports from the four testteams who have tested the various functions of the firewalls.

Testteam 3 (SNUS)

Scope
We have performed positive and negative tests. All of the tested firewalls did resist all attempts of penetration performed by existing and specially produced cracking-tools. However all firewalls can be set out of function by so-called denial of service attacks.

The tests of functionality showed that all systems had at least one incorrect setting. Among the problems discovered were faulty information in DNS, non-working FTP, no possibility to update web-sides, no ping-possibility and no news.
Settings, versions of operativesystems, choices of system-applications for mail, news, web, hardware, architecture and configuration are factors that all have an effect on the endurance and availability of the firewall.

Proxy and packetfiltrating
A firewall with *proxy-services* controls the flow of application traffic. I.e; the firewall+proxy let mail and news through but stops telnet and ftp-traffic. One way of attacking that type of firewall is to send great amounts of information which eventually will lead to a breakdown of the firewall.

In *packetfiltrated* systems it was more difficult to attack the firewallcomputer itself. On the other hand it´s possible to reach certain exposed machines on the net which are situated "inside the net". For example services such as mail, news and web. If one with appropriate tools or correct instructions how to crack or knock sendmail, NCSA, httpd, Microsoft Internet Informations server or similar "great" programs with documented security lapses out, well, then one has been able to penetrate the firewall.

Testteam 1 Combitech Nexus
Commercial firewalls has been proved to be relatively secure in regards of intrusions, but they often have faults which make them sensitive to blocked attacks. These errors often rely on the underlying operativesystems and not on the code of the firewall itself. Except for the construction of the firewall the underlying operativesystems and the competence of those who administrate and install it is of great importance.

Testteam 2 MedCom
This team ran the Internet security scanner (ISS) on four of the firewalls and received three vulnerable risks:
1) Routed service active (minimal risk)
2) Finger output risk (low risk)

The routed service risks are:
This provides an intruder with routing information. It opens up the possibility that an intruder can send false RIP packets causing your data to be routed to the intruder´s machine and thus being compromised.

The finger output risks are:
Finger gives an intruder information such as login accounts and trust hosts.

Testteam 4 Säkdata
With simulation of attacks from internet via a simulator (ISS), we found a few weaknesses. These could be fixed by a reconfiguration of the operating system of the firewall´s computer and also of the firewall itself.

ELECTRONIC MAIL/E-MAIL

Interoperability between electronic mail systems has become more important since many companies and organizations found that they have several incompatible email systems.

One solution to this problem is to design a mail backbone that can transport RFC822 & 821 +(MIME). Then several mail clients, servers and gateways can be connected to this backbone.

RFCs 822 and MIME
RFCs 822 & 821 are the specification for transport mechanism and messaging format for the mail system we know as email. MIME (Multipurpose Internet Mail Extensions) is a supplement to email that is needed in Sweden in order to exchange text, pictures etc under control of special rules. The test was divided into four parts: Minimal MIME (M) functions for Swedish language (SM) MIME and non-MIME functions (EN).

We tested 48 functions that comply with SMTP, MIME and interpretations by SNUS. Seven of the ten products that entered passed the test for minimal requirements for mime-functionality in Sweden. See table below:
This year we have tested several types of software components such as:

* Gateways, X400 - SMTP, (GW)
* MTA, (MTA)
* Mail clients, (C)

At the test 1996, the following companies participated:

No	Company	Products	Software	Result
1.	Des Communications	Borderware Firewall Server 3.1.1		
2.	GE Info Services	Business Network 2.3		
3.	ICL Networking	EMBLA 1.2	C	Passed
4.	Matti Aarnio, FUNET	Zmailer 2.99.27	MTA	Passed
5.	Microsoft AB	Microsoft Exchange Server 4.0(build 4.0.837.0)	C/MTA	Passed
6.	Netgain	Netgain Mimetic 2.0	MTA/G	Passed
7.	SUN Microsystems	Pronto E-mail 2.0.1		
8.	SUN Microsystems	Solstice Internet Mail client 0.9	C	Passed
9.	TeamWARE	Internet Mail V5	C	Passed
10.	Tele2	ADMD InterX X.400-to-Internet Gateway	C/MTA	Passed

ATM LAN - EMULATION

ATM LAN emulation is a way of simulation a LAN over The ATM network by using the current LAN standards like IEEE 802.3 and IEEE 802.5. The two IEEE protocols can operate over an ATM network via the ATM LAN emulation protocol.

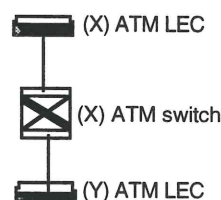
The basic function of ATM LAN emulation protocol is to resolve MAC addresses into ATM addresses. It is a protocol for MAC bridging (switching) over an ATM network. ATM LAN emulation uses the same drivers as existing MAC protocols. It means no changes of the higher level protocol in order to operate within an ATM network. We can have more than one VLAN within an ATM network.

7 companies with 17 products participated in this years LAN emulation interoperability tests.

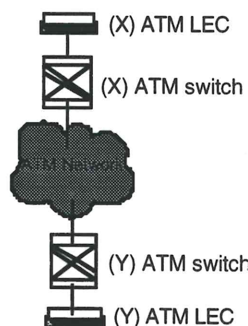
This test was done in several steps (1- 4).

Step 1, Two and two tests with different vendors
The test purpose is to establish contact between Y and the LECS, BUS, LES services in the ATMswitch. This gives us the opportunity to check, which VLAN Y is connecting. We will receive the LES and BUS services for our VLAN. The next part of the test is to establish contact with the other point Z.

Step 1 and 2



Step 2+ and 3

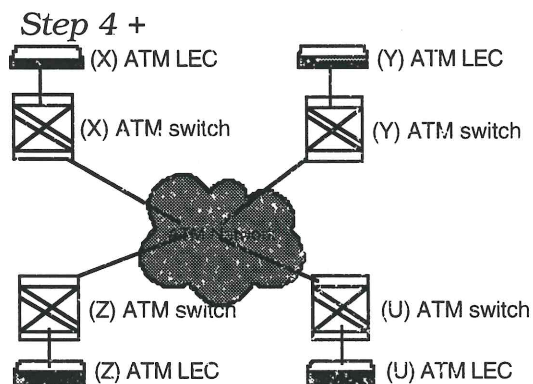


Step 2, Switch the vendor of the ATMswitch
Y and X will switch location and follow the procedure as step 1 describes.

Step 2+, Double ATMswitches
Both X and Y are setting up ATMswitches in the ATM network. The two ATMswitches connect via IISP protocol or well known ATM address. The X and Y accessproducts test against the ATM network.

Step 3, More accessproducts
X has an ATMswitch in the ATMnetwork, and more accessproducts vendor connects via X, Y, etc.

Step 4+ More ATMswitches
This will be an multi-switched ATM network. The network has many different ATMswitches connected with the UNI to NNI (IISP) protocol or Wellknown ATM address.



The conclusion is that almost every ATM LEC interope with the tested ATM services provided in the ATM network. The problems inflicted in the ATM LAN emulation test depends rather on the ATM LAN emulation configuration than a mismatch in the ATM LANE phase 1 standard. The ATM Forum phase 1 works well according to our tests especially the ATM LAN emulation clients.

Please read more about details on which products had interoperability functionality with one another in part 3:3.

IT-COUNTRY

Introduction

Interoperability in Sweden started in 1991 by testing base communication products for interoperability. Most of the companies that market these products have proved that they can set up and test communication products for infrastructure such as: routers, hubs, NMS-stations, LAN and serial links for various protocols today.

The general trend today is that many users prefer total solutions rather then building the infrastructure from different parts. This new requirement means that a vendor not only has to get the infrastructure to work for the customer but also a number of general functions such as: mail, www, ftp, telnet, news etc.

The interoperability tests in IT-Country were therefore on a function (application) level. Participation in IT-Country meant that one or two vendors got together to build an infrastructure. The task was to run applications in a booth, in order to run a model-company signifying a "real company". The two vendors could select any brand of product, the requirement was to perform the six functions that are specified in the test specification for IT-Country. (mail, www, ftp, telnet, news)

Our intention with IT-Country was to build a model of how Internet in Sweden will work in the nearest future. That is a secondary GIX-point, multiple connections, routing with BGP4, anonymous systems etc.

Purpose

Three IP-operators, Tele2, Telia and Global One provided access to the network and to Internet during the event. The condition for connections were the same as these IP-operators market in Sweden. IT-Country consisted of 18 model-companies built by 23 participating companies. Model-companies could be in three different sizes and complexity and the participants were free to chose the size, name and equipment of their company.

Realization

SNUS provided the opportunity for the participants to test their individual products in product tests which were conducted from January to April. Tested products 1996 were firewalls, mail-systems, and ATM/LAN-emulation equipment, see section 2. IT-Country was built on one week. The infrastructure and network were built on May 6 by the IP-operators and SNUS-NOC. The tests ran the 8th,9th and 10th of May. Some participants arrived late with their equipment and could therefore not participate fully in the test.

Test result
This was the first year of testing functions on an infrastructure. We found that one has to be very specific in the test procedure and we also learned that the level of specification need to be very precise. A majority of the companies participated in the tests that were performed.
Due to lack of time we decided together with the modelcompanies not to include news in the IT-Country-tests.

Mail
The test contains two parts we publish two test results. The first (table 1) presents the CC: results which show if the model-company have sent test mail or not.
The second (table 2) presents the FORWARD: which shows if test mail has arrived to the specified destination. We know that it has done so since the mail has been forwarded to SNUS NOC.

Ftp
The test specification was not specific enough on where the modelcompanies should put their FTP-files. Several copies were placed as files at the NOC, their own and other companies incoming area.
Many of the participants seem to have managed to fetch files and drop files from each others FTP-servers, and placed copies on the NOC server.
Since the test specification wasn't specific enough the result at the NOC ended up in a big mess with no order who did what. Therefore we won't present any table to this test.

WWW
Those who participated succeeded in this test and are marked with an x in table 3, Those *not* marked with an x in table 3 did not *fail* to complete the test but due to difficulties mentioned below they didn´t obtain contact.

- DNS configurations
- The internet providers had connectivity problems
- Firewall filtering. Didn't allow different traffic to go through (Mail, Ftp, WWW)

Summary
During this test the participants have proved that they are very good at setting up these types of services, and they are also well aware of the different problems that usually occurs. Therefore we think that the real life customer can benefit from fast installations and services from companies that handle these services in the future.

THE INTERNETDAY

Introduction

The Internetday was for the first time carried through during Interoperability-96. During the third day vendors and staff opened up for a wider range of public than those who visited Interoperability-96. They had an opportunity to take part of the results of the tests carried out during the first two days.

The targetgroup was people working with datacommunication but maybe not on such advanced level as those normally visiting Interoperability. Also those not able to spend two whole days for the event. Here they had a possibility to get a short presentation of the results. Customers of the exhibitors were invited to check on their suppliers competence and ability to perform the tests. Invited were also creators of public opinions and others competent to make decisions.

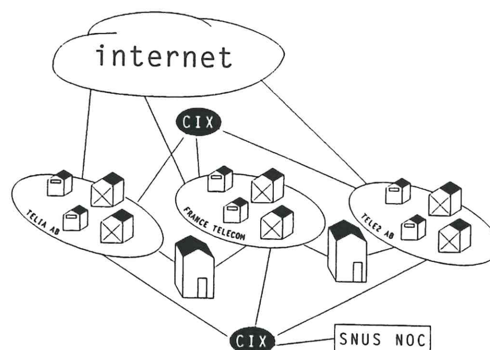
Purpose

The idea of a third day - the Internetday - came originally from some of the vendors/exhibitors participating in the Interoperability tests.
The purpose was to spread the facts and knowledge from the Interoperabilitytests to a wider range of people.

Realization

The visitors were provided with a pedagogical map and information about "IT-Country" built during the first two days. Short presentations of interesting subjects and testresults were held regularly and the public were also offered guided tours. The main idea was to show what worked and not worked in IT-Country in an easily understood way.

The results were also presented to people competent to make decisions from organizations and companies and a VIP-lunch was arranged. This to show effective ways of building internet-services at their respective organization. Approximately 400 persons attended the Internetday between 9 am - 3 pm.



3:1 BRANDVÄGGAR/ *FIREWALLS*

Testledare/Testmanager:
Staffan Hagnell, Network Management

Sidor/*Pages:*
19

Deltagare/Participants:	*Produkt/Product*
Cisco Systems	PIX
Combitech Nexus	TIS Gauntlet, version 3:1
Digital	Digital Firewall for Unix, version 2.0
DES Communications	BorderWare Firewall, Server version 3.1.1
Exo Data	TIS Gauntlet, version 3:1
Media Communications	TIS Gauntlet, version 3:1
Salcom	Firewall-1, version 2.0c
SUN	Firewall-1, version 2.0

3.1 Test av Brandväggar/Firewalls

Innehåll

1. INLEDNING

Intresset för säkerhet inom Internet ökar, inte minst på grund av de intrång som inträffat de senaste sex månaderna. Det finns en rad funktioner som skyddar användare i en organisation från attacker från omvärlden och flera företag bygger upp brandväggar för att skydda sina interna nät (Intranet). Vi har använt benämmningen brandvägg på de samlade funktioner som skyddar interna nät.

Årets Interoperabilitetstester har genomförts av SNUS, under ledning av Staffan Hagnell, Network Management, i samarbete med Säkdata,Cisco Systems, Combitech Nexus, Digital Equipment, DES Communications, ExoData, Media Communications, Salcom och SUN.

Testen inleddes i januari-96 med att de svenska företag som säljer firewallutrusning bjöds in att delta. Flera företag erbjuder firewallprodukter, konsulttjänster och även testverksamhet av firewalls.

För att få bra förutsättningar för testen upprättades tidigt en testspecifikation, konfiguration samt policy för hur testen skulle bedrivas. (se punkt 6)
12 företag hade bjudits in, 8 företag genomförde testen.Testresultaten finns i de enskilda testgruppen 7.1-7.4 och i testrapportens inledande "summary".

2. DELTAGARE

Företag	Produkt	Kontaktperson <epost>
Cisco Systems	PIX	Göran Nordström <gnordstr@cisco.com>
Combitech Nexus	TIS Gauntlet version 3.1	Nils Daniels <Nils.Daniels@Nexus.SE>
Digital	Digital Firewall for Unix version 2.0	Sören Altemark <Soren.Altemark@soo.dec.com>
DES Communications	BorderWare Firewall Server version 3.1.1	Benny Hansson <benny@descom.se>
ExoData	TIS Gauntlet version 3.1	Lars Rosenkvist <lars@exodata.se>
Media Communications	TIS Gauntlet version 3.1	Pär Ahrén <pera@medcom.se>
Salcom	Firewall-1 version 2.0c	Åke Wallin <Johan@Salcom.se>
SUN	Firewall-1 version 2.0	Bertil Lindblad <Bertil.Lindblad@sun.se>

3.TESTLEDARE

Staffan Hagnell, Network Management, <shl@netman.se>Patrik Carlsson, Network Management, <patrik@netman.se>

4.TESTLAG

Testlag 1	Combitech Nexus	Thomas Törnblom <Thomas.Tornblom@Nexus.SE> Thomas Holmström <Thomas.Holmstrom@Nexus.SE> Mikael Kuisma <Mikael.Kuisma@Nexus.SE>
Testlag 2	MedCom	Pär Ahreén <pera@medcom.se>
Testlag 3	SNUS	Martin Fredriksson <emwmf@emw.ericsson.se> Ilje Hallberg <iha@incolumitas.se> Robert Malmgren <rom@incolumitas.se> Tomas Olovsson <olovsson@ce.chalmers .se> Jan Michael Rynning <jmr@incolumitas.se >
Testlag 4	Säkdata	Anders Sandell <anders.sandell@sakdata.se>

5. GENOMFÖRANDE

Under vecka 16 (15-19 april) 1996, testades följande leverantörers brandväggar:

- DES Communications
- Salcom

Under vecka 17 (22-26 april) 1996, testades följande leverantörers brandväggar:

- Cisco Systems
- Combitech Nexus
- Digital
- ExoData
- Media Communications
- SUN Microsystems

6. TESTSPECIFIKATION

6.1 Konfiguration

Brandväggen ska ha en anslutning till ett inre och ett yttre nät. Båda dessa nät är Ethernet.

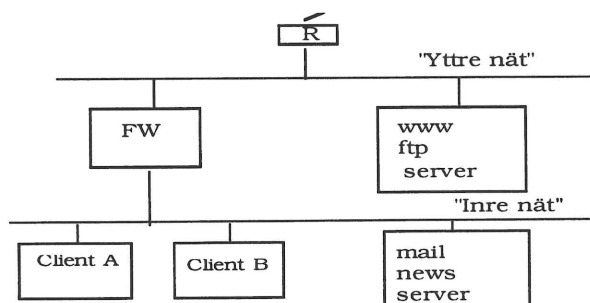
6.1.1 Anslutningar till det inre nätet

Till det inre nätet ansluts:

en mail-server, tillhandahålls av testledningen
en news-server, kan som option tillhandahålls av testledningen
en klient A som ska beredas åtkomst till Internet
en klient B som inte ska beredas åtkomst till Internet

Host	**IP-adress**
FW-internt interface	10.1.1.1
mail	10.1.1.10
news	10.1.1.10
client A	10.1.1.20
client B	10.1.1.21

Principkonfiguration



Subnetmask för det inre nätet är förslagsvis 255.255.0.0. Om proxy inte hanteras, anges detta och nya adresser ges.

6.1.2 Anslutningar till det yttre nätet

Det yttre nätet ansluts till Internet.

Ange hur många officiella IP-adresser som behövs.

6.1.3 Utrustningslista

Testarna ska ta med:

1 st Firewall
1 st Extern DNS-funktionalitet
1 st Extern WWW-funktionalitet
Eget kablage
Egna grenuttag

6.2 Säkerhetspolicy för brandväggstesterna

6.2.1 Tjänster som tillhandahålls åt omvärlden

6.2.1.1 DNS

A-records ska tillhandahållas för följande;

- ns.XXX.netman.se
- mail.XXX.netman.se
- www.XXX.netman.se
- ftp.XXX.netman.se

MX-records ska tillhandahållas för följande:

- XXX.netman.se Där XXX ges ett unikt värde för varje testdeltagare. OBS!

6.2.1.2 WWW

En WWW-server ska tillhandahållas för användarna i omvärlden. Informationen i denna server ska kunna uppdateras från insidan. Ange hur uppdateringen sker!

6.2.1.3 FTP

En FTP-server ska tillhandahållas för användarna i omvärlden. Informationen i denna server ska kunna uppdateras från det inre nätet. Ange hur uppdateringen sker!

6.2.2 Informationsutbyte med omvärlden

6.2.2.1 Epost

Epost ska kunna tas emot och skickas från en smtp-server placerad bakom brandväggen(inre nätet).

6.2.2.2 News

Som option, ska news kunna tas emot till och skickas från en news-server placerad bakom brandväggen. Extern newsfeed är 194.52.54.41

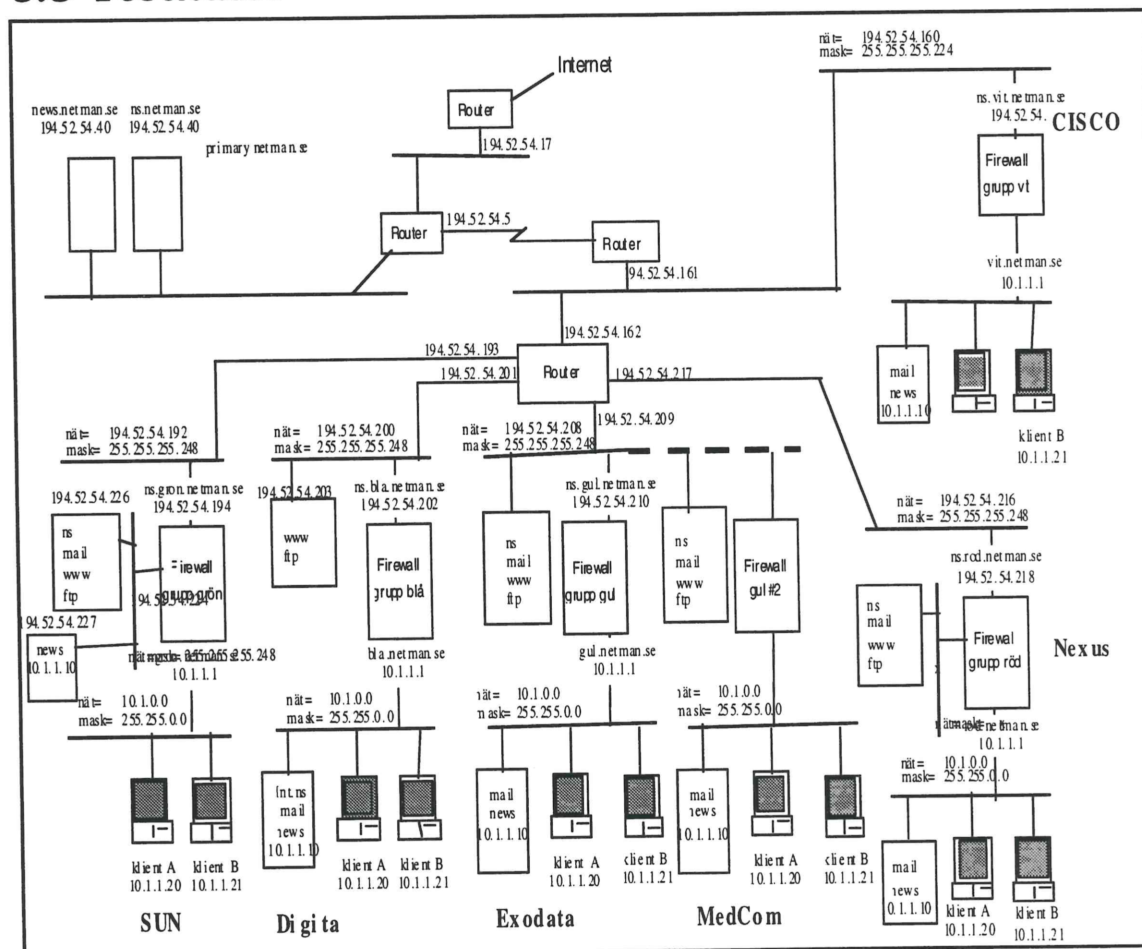
Om annan lösning förordas för att erbjuda användarna news, beskriv vilken.

6.2.3 Tjänster tillgängliga för användare på det inre nätet

Följande tjänster ska erbjudas användare på client A på det inre nätet via firewall ut mot Internet:

WWW, Gopher, FTP, Telnet, Ping, Firste Class, Real AudiIdentifiering av användare på client A ska i första hand ske på användar identitet. Om detta inte är möjligt får som andra hands alternativ identifiering ske på IP-adress.

6:3 Testnätet



6.4 Etik och policy för brandväggstesterna

Innan testerna inleddes enades deltagarna om följande förhållningsregler:

- Testresultat får inte spridas före Interoperabilitet 1996, 8 maj 1996
- Eventuella säkerhetsproblem som upptäcks ska omgående meddelas leverantören.
- Leverantören ska erbjudas tillfälle att kommentera eventuella brister i sin produkt, då testresultaten kungörs.
- Leverantören måste få tid för att rätta till fel och distribuera ut ny programvara till sina kunder innan detaljerad information om ett eventuellt fel sprids.
- Vid en eventuell tvist om testresultat mellan testare och leverantör ska testledningen kunna kontrollera testen
- Brandväggen får inte konfigureras om under testen. Eventuellt kan testare och leverantörer komma överens om att detta ska ske.
- Konfiguration av brandväggen ska publiceras offentligt.
- Attacker för att testa förlust av tillgänglighet får utföras. Dock får elsladden endast ryckas sparsamt.

7.0 TESTRESULTAT

7.1 TESTRESULTAT - TESTLAG 1 COMBITECH NEXUS

Detta dokument är en övergripande beskrivning av resultat som framkommit under de tester av brandväggsprodukter som Combitech Nexus deltog i inför Interoperabilitet-96. Dokumentet speglar endast de av Combitech Nexus utförda testerna.

7.1.1 Ordförklaring

Brandvägg är strikt sett en inadekvat benämning av de produkter vi testat. En brandvägg är en konstruktion för att skydda ett internt nät mot otillbörlig åtkomst från externa nät. Denna konstruktion kan bestå av ett antal olika komponenter, så som applikationsgateways, ip-filter etc. De produkter vi testat är paketerade lösningar som används vid konstruktion av en sådan brandvägg mot yttre nät. Vi kommer dock för enkelhets skull, efter detta klargörande, kalla dessa produkter för *brandväggar* i detta dokument.

DMZ, DeMilitarized Zone är här en benämning på nätverket mellan ISP-routern (IP-operatörens router) mot omvärlden och brandväggen. Externt eller yttre nät används här synonymt.

Dolt nät, inre nät är näten som skyddas, normalt det företagsinterna nätet.

ISP - Internet Service Provider, det företag som levererar Internet-tjänsten.

ARP - Address Resolution Protocol, en mekanism för att koppla ip-adresser till motsvarande mac-adresser.

7.1.2 Förutsättningar

Varje brandvägg sattes mellan ett publikt nät(yttre nät)och ett eller flera dolda nät(inre nät) på dess inre interface. På detta/dessa dolda nät sattes servrar och klienter upp för att uppnå funktionen enligt testspecifikationen. I korta drag gick den ut på att erbjuda clienter på insidan transparent åtkomst till de vanligaste tjänsterna (smtp, http, ftp, gopher, real audio, telnet m.fl.) samt tillåta extern åtkomst av interna servrar för http, gopher, ftp etc. Testerna pågick under två veckor, vilka blev förlängda till tre. Tredje veckan hade dock inte Combitech Nexus någon möjlighet att deltaga.

7.1.3 Val av tester

Med hänsyn till den begränsade tiden som fanns för testerna samt att testmiljön var något artificiell, koncentrerade vi testerna till punktangrepp på känsliga punkter i stället för att göra en komplett analys.
På grund av att brandväggarna främst är starka på tcp/ip-nivån för filterfunktioner, och på applikationsnivån för proxies, försökte vi påvisa svagheter i överliggande respektive underliggande nivåer.
Vid utvärdering av brandväggar är saker som prestanda, funktionalitet, användarvänlighet etc naturligtvis av mycket stor betydelse. Combitech Nexus har dock inte utfört några sådana tester inför Interoperabilitet-96.

Notera att dessa begränsade tester inte ska förväxlas med Combitech Nexus IT-säkerhetstjänst, Säkerhetskontroll av internetanslutning, vilken bland annat inkluderar penetrationstest.

7.1.4 Val av testverktyg

På grund av testernas speciella natur, kommer man inte långt med de publikt och kommersiellt tillgängliga verktyg som finns, exempelvis SATAN och ISS. Dessa är främst avsedda att testa enskilda maskiner med avseende på kända säkerhetshål och inte brandväggar. I ett fall som detta, gick vi i princip enbart på egenutvecklade verktyg och testmetodiker.

7.1.5 Testade produkter

- Borderware från DES Com
- Firewall-1 från Salcom
- Gauntlet från Exodata
- DEC Firewall for Unix från DEC
- Gauntlet från Combitech Nexus
- Pix från Cisco
  Pix från Cisco kunde inte testas på grund av frånvaro av klienter/sevrar bakom den. Tredje veckan kom sådana på plats, men tyvärr hade vi inte resurser för test då.
- Firewall-1 från Sun
- Gauntlet från Medcom

7.1.6 Testresultat

Här följer en sammanställning av de testade detaljer vi hittade som skilde i de olika brandväggarna. Diverse tester som inte gav intressanta resultat alternativt inte skilde de olika produkterna åt, är inte redovisade här.

7.1.6.1 ARP-attacker

Att injicera felaktig arp-information gav mycket intressanta fenomen. En sådan form av attack kan bara utföras under förutsättning att en annan maskin på samma IP-nät som brandväggen redan har infiltrerats, då arp inte är ett routingbart protokoll. Det kan exempelvis vara en yttre maskin för publik WWW eller routern som komprometterats. Om så, kan både blockerande attacker, övertagandet av sessioner och spoofing av mer eller mindre godtycklig applikationsdata utföras enligt nedan.

7.1.6.2 Överskrivning av arp-entry för yttre router

Genom att i brandväggen injicera en falsk arp-entry för ISP-routern, kan en inkräktare ta över all trafik från brandväggen genom att själv utge sig för att vara routern. Inkräktaren har då full kontroll över all trafik från den interna nätet mot internet. Samtliga brandväggar, utom Combitech Nexus Gauntlet, var känsliga för en sådan attack. Det enklaste sättet att förebygga attacken, är att vid installation av brandväggen använda ett statiskt arp-entry för ISP-routern.

7.1.6.3 Överskrivning av arp-entry för inre maskiner.

Främst en blockerande attack (denial-of-service). Om detta är möjligt, går det att ifrån DMZ styra om trafiken på det inre nätet, så att trafiken från brandväggen inte längre når rätt inre maskin. Generellt var samtliga brandväggar utom Digitals och Firewall-1 sårbara på detta område. Gauntlet med BSD/OS loggade dock händelsen, även om den inte förhindrade det.

7.1.6.4. Injicering av stora mängder arp-data

Vi testade även att fylla arp-tabellen med stora mängder nonsens, för att undersöka hur brandväggarna hanterade det. Under själva arp-bombardemanget stod alla brandväggar i praktiken still på grund av hög nätlast. Alla utom en Firewall-1 återhämtade sig dock efter någon minut efter att arp-sändandet upphört. Denna Firewall-1 frös istället ihop helt, och måste manuellt bootas om för att komma igång igen. Intressant är, att ingen brandvägg lyckades inse att de arp-paketen vi skickade var ren nonsens och omöjligen skulle kunna ha legalt sänts av någon maskin på det aktuella nätet.

7.1.6.5 TCP-attacker

Med hjälp av legal trafik i stora mängder går det i vissa fall att slå ut olika funktioner i brandväggen på grund av resursbrist i operativsystemet. Vi provade att öppna ett maximalt antal tcp-sessioner mot brandväggarna och maskiner bakom den. Här upptäckte vi en hel del intressanta fenomen. Under stressfasen blev samtliga brandväggar helt blockerade för övrig trafik.. Efter attacken var det endast DEC:s och Exodata:s brandväggar som återgick till normaltillstånd igen. Övriga var mer eller mindre permanent satta ur funktion. Allt från kraschade processer till kraschade diskar observerades. Efter modifieringar av konfiguration och/eller uppgraderingar av operativsystem uppnådde fler brandväggar bättre resultat.

7.1.6.6 Applikationsnivån

De filtrerande brandväggarna (Firewall-1 och DEC) ställer höga krav på att även den interna miljön innanför brandväggen säkras upp. T ex lyckades vi slå ut en mailserver som låg skyddad bakom en Firewall-1 utan större problem, och lyckades nästan penetrera en intern mailserver, vilket dock hindrades av en väl uppdaterad sendmail.

7.1.6.7 Slutord

Kommersiella brandväggar har visat sig vara relativt säkra mot intrång, men har ofta brister som gör dem känsliga för blockerande attacker. Dessa brister beror ofta på underliggande operativsystem och inte själva brandväggskoden.
Förutom brandväggens konstruktion har underliggande operativsystem och kompetens hos de som installerar och administrerar brandväggen stor betydelse för brandväggens funktion.

7.2 TESTRESULTAT - TESTLAG 2 MEDIA COMMUNICATIONS

7.2.1 Inledning

Medcom genomförde en kortfattad test av 4 st firewall's med Netcat och Internet Security Scanner (ISS). På grund av tidsbrist fick vi inrikta oss på ett snabbtest i stället för en fullständig Tigerteam test.

ISS och portscan är ett första steg i en total Tigerteam test och bör följas av ett antal andra tester också, såsom "denial of service" attacker. ISS var i denna version mer anpassad för "vanliga" UNIX maskiner. I den nya versionen finns mer av tester som har anpassats för brandväggstest samt Webserver test förutom de vanliga testerna.
Fördelen med s k automatiska verktyg (som ISS) är att man då på ett enkelt sätt kan köra testerna om igen då man har ändrat någon parameter i brandväggen.

I problematiken med brandvägg, TCP/IP, DNS, ta emot e-mail samt loggning ligger att man inte helt kan skydda sig mot avlyssning och "denial of service"-attacker då detta är ett arv från gamla tider då man gjorde program som <u>bara</u> skulle fungera utan att tänka på säkerheten...

- I IP (TCP & UDP) så finns det ett antal olika problem med avlyssning, spoofing, routing etc.
- Med loggning så kan man tillslut alltid fylla en disk så att maskinen stannar eller så att den tidigare loggen skrivs över om inte detta övervakas och åtgärdas i tid.
- Att ta emot e-mail gör en också mottaglig för att få disken fylld och maskinen stannar.

Avgränsningar i brandväggs testerna

Detta är inte riktigt representativa brandväggar då det inte fanns några krav på att man skulle släppa igenom en massa saker som alltid kommer upp att man bara "måste" släppa igenom som t ex:
"Du måste bara släppa igenom den här applikationen 'qzp' annars kan inte jag göra mitt jobb ..."

Klient maskinerna användes inte heller aktivt under testen så som det hade varit i en verklig situation.

(Man har här inte tagit hänsyn till att man kan kryptera och/eller autenticiera trafiken och på så sätt få säkrare uppkopplingar).

Följande funktioner ingŒr inte i testen:

- DNS uploads
- process/socket "denial of service"
- fylla hårddisken
- Route omställning

7.3.2 Netcat visar öppna portar för trafik genom firewall och gav resultatet:

Firewall A ns.rod.NetMan.SE [194.52.54.218]: 14 portar öppna

8000	(?)	- Gauntlet admin eller http-proxy
7777	(authsrv)	
7070	(ra)	
513	(login)	
119	(nntp)	
110	(pop3)	
80	(http)	
79	(finger)	
70	(gopher)	
53	(domain)	
43	(whois)	
25	(smtp)	
23	(telnet)	
21	(ftp)	

Firewall B ns.gul.NetMan.SE [194.52.54.210]: 15 portar öppna

8000	(?)	- Gauntlet admin eller http-proxy
7777	(authsrv)	
7070	(ra)	
513	(login)	
119	(nntp)	
113	(auth)	
110	(pop3)	
80	(http)	
79	(finger)	
70	(gopher)	
53	(domain)	
43	(whois)	
25	(smtp)	
23	(telnet)	
21	(ftp)	

Firewall C ns.gron.NetMan.SE [194.52.54.202]: 32 portar öppna

8319	(?)	
8318	(?)	
8317	(?)	
8316	(?)	
8315	(?)	
8314	(?)	
8313	(?)	
8312	(?)	
8311	(?)	
8310	(?)	
8080	(?)	Brukar vara http-proxy
6000	(?)	X11
3004	(?)	
1090	(?)	
1025	(?)	blackjack
672	(?)	
671	(?)	
670	(?)	

669	(?)	
668	(?)	
667	(?)	
666	(?)	doom eller mdqs
119	(nntp)	
79	(finger)	
53	(domain)	
29	(?)	msg-icp
28	(?)	
27	(?)	nsw-fe
26	(?)	
25	(smtp)	
23	(telnet)	
21	(ftp)	

Firewall D ns.bla.NetMan.SE [194.52.54.194]: 0 portar öppna

Timeout på alla portar (fågan är hur den ska ta emot tex mail ...)
Kan ha varit feluppsatt vid testen.

7.2.3 ISS visar följande

Total Number of Vulnerability Risks: 3

Routed service active [Medium Risk]: 1
Finger Output [Low Risk]: 2

ISS beskrivning av riskerna

Routed service active [Medium Risk]

This provides an intruder with your routing information. It opens up the possibility that an intruder can send false RIP packets causing your data to be routed to the intruder's machine and thus being compromised.

If you are using a simple gateway, you should just use a default route. Most sites are connected through a single point of entry to the Internet with a simple infrastructure. These sites do not need to run routed. Disable routed from running on the machine.

Min kommentar

Detta gäller i första hand vanliga UNIX maskiner då detta är något som BÖR vara åtgärdat på en brandvägg. Jag hann inte gå vidare och testa mer p g a tidsbrist.

Finger Output [Low Risk]

Finger gives an intruder information such as login accounts and trust hosts

Disable the finger daemon by commenting it out of /etc/inetd.conf and restarting inetd.

Min kommentar

I de fall då finger är aktivt på brandväggar är programmet utbytt mot ett annat som endast skriver ut en text så som:

To send e-mail to us use: surename.lastname@site.se

7.2.4 Ordförklaring

tjänst	betyder här en nätverks tjänst som t ex. e-mail, http, FTP etc
spoofing	en illasinnad person låtsas att vara en annan genom att han (sällan hon) sätter sin IP-adress till en som någon annan har och med hjälp av ett antal olika tekniker lurar andra datorer på nätet
"denial of service"	"förnekande av tjänst" betyder att någon har gjort en "tjänst" eller maskin otillgänglig.

7.3 TESTRESULTAT - TESTLAG 3 SNUS

Preliminär rapport från SNUS Brandväggstester 1996
Skrivet av Robert Malmgren och Ilja Hallberg.

7.3.1 Introduktion

De tester som utgick från den ovan angivna testspecifikationen var Real Audio och First Class. Orsaken till detta är att personen som åtog sig att skaffa servers och klienter till dessa tester inte höll vad han lovat, tester gjordes sŒledes pŒ www, gopher, FTP, Telnet pch Ping.

Rapportering av brandväggstesten är uppdelad i två delar, en med resultat från de praktiska testerna och en med detaljpresentationer av leverantörer och brandväggsprodukter.

7.3.2 Testteam

Testarna bestod av fyra testlag sammanlagt tre företag: - Säkdata, Combitech Nexus, Medcom samt testledning.

7.3.3 Testledning (SNUS) bestod av folk från olika företag

Ericsson Microwave Systems	Martin Fredriksson
Incolumitas	Ilja Hallberg, Robert Malmgren Jan Michael Rynning
Network Management	Patrik Carlsson, Staffan Hagnell
Carlstedts	Tomas Olofsson

Testledningen (SNUS) delade upp sig i tre grupper, Patrik Karlsson och Staffan Hagnell Network Management skötte infrastruktur med routers, internetanslutning, adressplan, administration, etc. Ilja Hallberg utförde tester för att se att leverantörerna fullföljde specifikationen gällandes vilka tjänster som skulle släppas igenom respektive hindras av brandväggen samt funktionstester. Övriga i testledningen utförde penetrerings och denial of serviceattacker (tillgänglighetsattacker) mot systemen.

7.3.4 Testledningens tester (SNUS)

Vi har utfört positiva och negativa tester. Resultatet är att samtliga testade brandväggar har stått emot intrångsförsök med existerande och speciellt framtagna crackingverktyg. Däremot gick alla system på ett eller annat sätt att sätta ur funktion genom sk denial of service-attacker. I de värsta fallet var man tvungen att ominstallera brandväggen eftersom filsystemet var korrupt.

Funktionalitetstesterna gav att alla systemen hade minst en eller flera felaktiga inställningar. Bland de problem som uppdagades var felaktig information i DNS, icke fungerande ftp, ingen möjlighet att uppdatera egna websidor, ingen ping-möjlighet, ingen news.

Inställningar, operativsystemsversioner, val av systemapplikationer för mail, news, web, hårdvara och arkitektur inverkar alla på brandväggens uthållig- och tillgänglighet.

Tester av brandväggsfunktioner, positiva tester

- Vi gjorde en enklare kontroll av utlovad funktionalitet i de olika testsystemen. Tjänsterna WWW, gopher, ftp, telnet, ping, News, Epost och Real Audio skulle göras tillgängliga för interna användare. Testerna av FirstClass genomfördes inte på något testsystem. Utåt skulle systemet leverera tjänsterna WWW, Epost och anonym FTP. Systemets egna WWW-sidor skulle kunna uppdateras från klienter på det inre nätet. DNS skulle finnas tillgängligt både mot det inre nätet och mot omvärlden. För de flesta testerna använde vi Netscape Navigator.

- Vi gjorde inga genomgående tester av konfigurationsverktygen och gränssnitten mot brandväggsprogramvaran, inte heller gjorde vi några kontroller av systemets konfiguration i övrigt. Flera system hade mycket eleganta användargränssnitt som gav intryck av att göra systemen lättskötta. Vi tycker inte att man får låta sig invaggas i en falsk säkerhet av att skötsel av ett brandväggssystem kan skötas utan kunskaper om hur systemet och nätverksprotokollen fungerar. (Grafiskt snygga logglistor med osorterad och ickefiltrerad information är kanske inte alltid det optimala verktyget för att utröna en attack omfattning och ursprung.)

- Överlag fungerade alla testade system bra. Nästan inget av systemen var felfria, men efter diskussioner med leverantörerna kom vi i de flesta fall fram till att det handlade om felkonfigurationer eller missförstånd angående testupställningen. De brister som upptäcktes var: fel konfigurerade ftp-demoner, ej komplett DNS-konfiguration, ej komplett stöd för RealAudio, bortfiltrering av utgående Ping, avsaknad av news.

- Kanske bidrog vetskapen om att systemen skulle testas till att de var lite väl hårt tillsnörpta. Som kund kanske man också kan dra slutsatsen att ett brandväggssystem inte installeras med komplett funktionalitet direkt på en dag. I diskussionerna med leverantörerna användes vid flera tillfällen den gemensamt framtagna kravspecifikationen/ test-beskrivningen. Vikten av en ingående kravspecifikation bör inte underskattas.

7.3.5 Negativa tester

Vi lyckades genomföra olika typer av sk "denial of service"-attacker mot samtliga system. Med denna typen av attacker mot ett system finns möjligheten att någon i organisationen som är mål bestämmer att brandväggen "inte fungerar och temporärt tar bort systemet för att den normala trafiken skall få komma fram.

Ett Gauntletsystem och Borderware-system krashade om man gjorde ett antal samtidiga firewalluppkopplingar mot flertalet vanliga tjänster. Gauntletsystemet skrev sönder filsystemet på ett sådant sätt att datorn inte kunde starta igen utan ominstallation. Både Borderwaresystemet och Gauntletsystemet var möjliga att ändra så att de kunde stå emot denna typ av attacker, antingen med uppgradering av programvara eller genom omkonfiguration. Såsom Borderware levereras möjliggör standard-inställningarna denna attack. Det som avhjälpte problemen för Gauntlet var uppgradering från BSDI 2.0 till version 2.1.

Ett annat Gauntletsystem blev i princip oanvändbart genom att vi skickade IP-trafik från icke-existernade avsändare och sedan kontaminerade vi ARP-cachen. Detta resulterade i att systemet loopade och pratade med sig själv, därmed fyllde den loggar, åt CPU-resurser och hade trasiga interna tabeller över IP och ARP.

Digital firewall for UNIX genererade ett larmbrev när någon försökte koppla upp sig mot en oanvänd port, tex en följd av använgning av sk portscanners. Dessa brev skickades vidare till en NT-server innanför brandväggen. När det skickades runt 20000 e-mail till NT-maskinen i rask följd så uppstod det något fel vilket gjorde att det uppstod fel i filsystemet på NT-servern. Resultatet av detta fel var att det inte gick att komma Œt någon fil i inboxen, och man kunde därmed inte se någon av de larmmeddelanden som inkommit.

I exemplet ovan var det Digital och NT, men vi har sett liknande konfigurationer i andra produkter och för andra operativsystem. Lärdomen av detta är att de larmsystem man installerat istället för att larma kan bidraga till den villervalla och de problem som uppstår vid ett intrång/intrångsförsök.

7.3.6 Arkitektur på brandväggssystem

Ett resultat av testerna var att skillnaden mellan paketfiltrerande brandväggar och brandväggar som bygger på applikationsproxy framstod mer konkret.

För den trafik som skulle släppas igenom brandväggen, exempelvis mail och news, så skyddade de system som byggde på proxyserver bakomvarande tjänster bättre. Samtidigt så fick brandväggsdatorn med proxytjänsterna ta smällen vid intrångsförsöket, vilket i flera fall resulterade i att brandväggsdatorn krashade. En ovetande brandväggsadministratör i en organisation med potenta chefer kan bli övertalad att koppla förbi en ständigt krashande brandvägg eftersom “den inte fungerar”. Det kan vara ett sätt att ta sig in, att genom utnötning se till att brandväggen tas ur drift.

I paketfiltrerande system var det svårare att ge sig på brandväggsdatorn som sådan. Däremot kan man komma åt vissa exponerade tjänster på maskiner på nätet “innanför” brandväggen. Exempelvis tjänster såsom mail, news och web. Om man med lämpliga verktyg eller rätt instruktioner för hur man crackar eller slår ut sendmail, NCSA httpd, Microsofts Internet Informations Server eller liknande “stora” program med dokumenterade säkerhetsluckor, - ja då har man nått in bakom brandväggen.

Flera av de proxybaserade brandväggarna hade svårt att erbjuda vissa typer av tjänster som var uppsatta i testspecifikationen beroende på att det inte fanns någon proxytjänst för just den typen av trafik. Det vanligaste exemplet var "ping" som använder sig av de två ICMP-pakettyperna echo request och echo reply. Gauntlet och Digital hade inte stöd för att släppa igenom ICMP trafik i de testade versionerna.

Erfarenheten av ovan ger att en bra säkerhetslösning kombinerar både någon typ av paketfiltrering och proxytjänster. Förutom detta gäller som vanligt att de bastionmaskiner (www, FTP-server) som man har, oavsett var de sitter anslutna, måste vara väl skyddade.

7.3.7 Bättre tester av brandväggar inför framtiden

- **Tidsbrist**
  1 vecka per brandväggsuppsättning (2 system första veckan, 6 system andra veckan) räckte inte till för att kunna göra en utförligt testning av funktionalitet, konfiguration och möjligheter till intrång. Den tid som går åt för leverantörerna att installera testsystem ökar med antalet understödda protokoll.

- **Bättre uppdelning av negativa och positiva tester.**
  De tester som provar funktionerna i systemet, positiva tester, görs snabbare och mer koncentrerat om man kan separera dem från negativa tester av typen tillgänglighetsförlust (denial-of-service) och försök till intrång. Om ett system ska testas i en vecka är det bättre att ägna de första 2 dagarna åt att testa funktionaliteten i systemet och ägna resterande tid åt att försöka knäcka systemet. Upptäcker man under det första testpasset att vissa tjänster inte tillhandahålls går det att korrigera konfigurationen innan det andra passet startar.

- **Tester av systemkonfiguration**
  En god ide kan vara att låta varje brandväggsleverantör göra en enklare demonstration av konfigurationsverktyg och gränssnitt innan funktionstesterna inleds.

- **Egna klienter för funktionstesterna.**
  Under årets tester kom vi överens om att varje leverantör ställde upp med klientdatorer för testuppställningen; i praktiken fungerade det inte bra. Det är bättre om testgrupperna har en egen klient med fast IP-nummer som används i alla system. Man byter lätt system genom attkoppla om nätverksanslutningen. Innan testerna startar gör man en generell överenskommelse om vilken programvara som ska användas på klienterna. Det är också bra om åtminstone två klientmaskiner testar av ett system samtidigt med olika programvara.

- **Leverantörerna måste lämna lösenord**
  I de fall då leverantören tillhandahåller tjänster som är lösenordsbundna måste lösenorden lämnas till testpersonalen. På ett system kunde funktionaliteten inte testas fullt ut pga. bristandeinformation från leverantörens sida.

- **Fler funktioner?**

Ytterligare protokoll och tjänster kommer kanske att bli aktuella. Det kanske kan vara intressant att ställa frågor till leverantörerna om mer speciella lösningar. Tex. ett företag som vill att säljare ska kunna kontakta sitt huvudkontor med en "telnet"-liknande tjänst utifrån, eller att anställda på ett företag ska kunna köra X11-program på sina fältklienter mot interna servrar via brandväggen.

Hur viktig är fjärradministrationen av brandväggar? Ökar det risken för attacker som skapar tillgänglighetsförluster? Hur lätt är det att ta över eller avlyssna en klient som körfjärradministrationsprogramvaran?

- **Olika deltagarkategorier**

Beroende på hur brandväggsprodukterna på marknaden utvecklas kan det bli intressant att dela in leverantörerna i två eller fler deltagarkategorier med avseende på testningen av funktionalitet. Tex. kan man dela upp testningen i en avancerad och en enklare grupp. Detta beror av hur mycket resurser leverantörerna tycker att de kan lägga ned på ett testsystem. I den mer avancerade kategorin kan man testa virtuella nät, interna brandväggar, funktioner som analyserar inkommande data efter fientliga binärer.

Anonymous FTP [Low Risk]: 0
Netbios SMB Root Share [Medium Risk]: 0
Netbios SMB Dot Dot Bug [Medium Risk]: 0
Netstat [Low Risk]: 0
Sysstat [Low Risk]: 0
Bootparam [Low Risk]: 0
BootparamDom [Low Risk]: 0
Finger [Low Risk]: 0
Rusers Output [Low Risk]: 0
Finger Output [Low Risk]: 2

7.4 TESTLAG 4 - SÄKDATA

7.4.1 Förutsättningar

Säkdatas bidrag till SNUS Firewalltester bestod i att utföra attacksimuleringar. Dessa simuleringar utfördes från Säkdata via Internet med hjälp av verktyget Internet Security Scanner (ISS).

Vi har här valt att presentera de brister eller svagheter som vi fann i brandväggarna. De brandväggar som inte visade några tecken på svaghet vid attacksimulering med ISS har inte tagits med i denna redovisning.

Alla svagheter som vi lyckades spåra upp är resultat av felkonfigurerade operativsystem, samtliga går därför att rätta till genom att konfigurera maskinerna annorlunda.

Frågor och synpunkter kan lämnas per e-post till Anders Sandell, Säkdata AB.

7.4.2 Testresultat

Digital

Under testet indikerade ISS att Routed var startad på brandväggen. Routedkan lämna ut routinginformation till en potentiell inkräktare samtidigt som denne kan skicka in falska RIP-paket för att ändra brandväggens routingfunktioner.Enligt Digital själva var denna funktion konfigurerad på ett sätt somomöjliggjorde manipulation, detta har dock inte kunnat verifieras.På Digital:s brandvägg var även följande portar öppna:

666 (doom)
53 (domain

Tjänsten domain svarar på DNS-frågor från omvärlden och bör finnas där.På port 666 finns normalt tjänsten doom, men där hade Digital en tjänst autenticering.

TIS Gauntlet (Exodata)

Följande portar var öppna
513 (login)
53 (domain)

Tjänsten login används för fjärrinloggning med kommandot rlogin. Viss autenticiering utförs, det finns dock dokumenterade brister i denna för bland annat SunOS. Login skall vara avstängt på en brandvägg.

TIS Gauntlet (Nexus)
Följande portar var öppna:

513 (login)
53 (domain)

Som tidigare nämts skall tjänsten login vara avstängd på en brandvägg medan domain skall finnas där för att svara på DNS-frågor från Internet. Som parentes kan nämnas att denna Gauntlet-installation även hade Ident igång vilket medger viss spårning av TCP-kopplingar.

3:2 ELEKTRONISK POST/EMAIL

Testledare/Testmanager:

Patrik Fältström, Bunyip
Lars-Johan Liman, Sunet, KTH

Sidor/*Pages:*
19

Deltagare/Participants:	*Produkt/Product*
DES Communications	Borderware Firewall Server 3.1.1
GE Info Services	Business Network 2.3
ICL Networking	EMBLA 1.2
Matti Aarnio, FUNET	Zmailer 2.99.27
Microsoft AB	Microsoft Exchange Server 4.0(build 4.0.837.0)
NetGain	NetGain Mimetic 2.0
Sun Microsystems AB	Pronto E-mail 2.0.1
Sun Microsystems AB	Solstice Internet Mail client 0.9
TeamWARE Group	TeamWARE Internet Mail V5
Tele2	ADMD InterX X.400-to-Internet Gateway

3.2 Test Electronic Mail

1 Overview

1.1 History

The Internet suite of standards contains a number of standars regarding Internet electronic mail (e-mail) messages. A few of the more important ones are
RFC-821, Simple Mail Transfer Protocol, which regulates the most common way of transferring mail messages between hosts.

RFC-822, Standard for the Format of ARPA Internet Text Messages, which regulates the format of the contents of an Internet e-mail message.

RFC-1123, Requirements for Internet Hosts -- Application and Support, which contains amendments to a number of RFCs, among them 821 and 822.

RFC-1521, MIME (Multipurpose Internet Mail Extensions) Part One, which regulates ways of tagging and coding the information in messages bodies. This facilitates transfer of data other than English text.

RFC-1522, MIME (Multipurpose Internet Mail Extensions) Part Two, which regulates ways of tagging and coding the information in the message headers. This allows a variety of character sets to be used in header fields.

The Swedish Network Users' Society (SNUS) wants to encourage the use of these modern standards, and by performing the following tests during the Interoperability Fair 1996 in Stockholm, Sweden, and by issuing "SNUS certification" for software meeting these requirements, we hope to inspire software developers and vendors to strive towards interoperability in a standardized way.

2 The tests

2.1 Goals and Objectives

The goal of these tests is to prove the ability to send more complicated electronic mail than pure English text between applications conforming to the standards above.

Products conforming to the standars, and fulfilling the additional requirements set up by SNUS, will be awarded SNUS certificates for use within Sweden. SNUS has no authorisation to deny use of other software, but our hope is that this certificate will serve as a hint to the user community that the product in question meets certain basic requirements which may be considered important for smooth e-mail interaction in Sweden.

We also want to make a brief summary of the availability of optional MIME functionality in each product, to aid customers wanting to compare MIME software.

The tests should be viewed as technical, and the emphasis is on the software's behaviour towards the rest of the Internet, and on the correctness of the final contents of the mail messages. Many aspects of mail software must be regarded as matters of taste, and we have tried to avoid those, and to concentrate on qualities that can be measured in an objective manner.

2.2 Test managers

The following persons will represent SNUS in the mail tests.

Patrik Fältström
Responsible for MIME tests.
Program Manager - Distributed Services
Bunyip Information Systems Inc.

Lars-Johan Liman
Responsible for RFC-822 and SMTP tests.
Research Engineer
Royal Institute of Technology, Network Operations Centre

L-H Carlsson
Network Consultant
Network Management OSI AB

Assar Westerlund
Systems Administrator
Royal Institute of Technology, Center for Parallel Computing

When sending test messages, please use the email address:
mime-test@cafax.se

If you don't, your tests will be mixed with our ordinary mail which will make it very difficult for us to handle it in a proper way.
For questions about the tests, discussions about MIME etc, please contact the test leaders using e-mail, addressed
mime-group@cafax.se

To reach all participants in the MIME test, please use the address
mime-participants@cafax.se
Our individual mail addresses are:
Patrik Fältström: paf@bunyip.com
Lars-Johan Liman: liman@sunet.se
L-H Carlsson: hockey@netman.se
Assar Westerlund: assar@pdc.kth.se

2.3 Participants

At the tests 1996, the following companies participated:

1	DES Commmunications	Borderware Firewall Server1	3.1.1
2	GEIS Sweden	Business Network	2.3
3	ICL	EMBLA	1.2
4	Matti Aarnio, FUNET	Zmailer	2.99.27
5	Microsoft AB	Microsoft Exchange Server	4.0 (build 4.0.837.0)
6	NetGain	NetGain Mimetic	2.0
7	Sun Microsystems AB	Pronto E-mail	2.0.1
8	Sun Microsystems AB	Solstice Internet Mail client	0.9
9	TeamWARE Group	TeamWARE Internet Mail	V5
10	Tele2	ADMD InterX X.400-to-Internet Gateway	

The participating software packages were so different in functionality, from gateways between X.400 and SMTP, via MTA's to pure email clients, so comparing the different products in this test is only possible in a very few cases. The reader have to instead use this result as a description of the software itself when comparing with other software packages available on the market.

Specification of the tests done can be found at http://www.cafax.se/MIME-tests.html, and the result itself can be found in the table below.

As of June 14, 1996, these results are very preliminary and will most definitely change. The respective companies have not had time to themselves check these results and/or come with comments. When the final result is available, that will be announced separately.

2.3.1 Contact information:

DES Communication
Name of product: Borderware Firewall Server
Version: 3.1.1
Manufactured by: Border Network Technologies Inc
Tested on platform(s): Intel
Available on platform(s): Intel
Availablility: Yes
Comments: We are testing the SMTP/POP3 server only on the Borderware product, but we use Microsoft Exchange 4.0 for Windows 95 for the other parts.

Form completed by: Benny Hansson
Email: benny@descom.se
Phone: +46-8-969201
Fax: +46-8-968338
Address: Orrvägen 26

GEIS Sweden
Name of product: Business Network
Version: 2.3
Manufactured by: GE Information Services
Tested on platform(s): Win95
Available on platform(s): DOS, Win 3.x, Win95 WinNT, Mac
Availablility: Worldwide through GEIS
Form completed by: Rolf Schutz
Affiliation: GEIS Sweden
Email: Rolf@GEIS.GEIS.com
Phone: +46-8-4579581
Fax: +46-8-4579580
Address: St. Eriksg. 117
Sales contact: See above

ICL
Name of product: EMBLA
Version: 1.2
Manufactured by: TeamWare Group AB
Tested on platform(s): Windows 3.1X, Windows NT, Windows 95
Available on platform(s): Windows 3.1X, Windows NT, Windows 95
Availablility: Now
Comments: POP/IMAP-client
Form completed by: Peter Jervgren
Affiliation: ICL
Email: peter.jervgren@pro.icl.se
Phone: +46-13-31 70 00
Fax: +46-13-31 74 60
Address: TeamWare Group AB
Box 1938
S-581 18 Linköping
Sweden
Sales contact: Lars Hagberg
Affiliation: ICL
Email: marcomms@pro.icl.se
Phone: +46-13-31 70 00
Fax: +46-13-31 74 60
Address: Box 1938
S-581 18 Linköping
Sweden

Matti Aarnio, FUNET

Name of product: ZMailer
Version: 2.99.27
Manufactured by: the author(s)
Tested on platforms: Several UNIXes
Available on platforms: Several UNIXes
Availability: ftp://ftp.funet.fi/pub/unix/mail/zmailer/
Comments: Free software, support available
Form completed by: Matti Aarnio <mea@nic.funet.fi>
Affiliation: current author
Email: Matti Aarnio <mea@nic.funet.fi>
Phone: +358-50-558-1790
Sales contact: the author -- if you want to buy customization/support

Microsoft AB

Name of product: Microsoft Exchange Server
Version: 4.0 (build 4.0.837.0)
Manufactured by: Microsoft Corp.
Tested on platform(s): Windows NT Server 3.51 and Windows NT Server 4.0 Beta II
Available on platform(s): Clients on Windows 95, Windows for Workgroups 3.11, Windows NT 3.51 and Windows NT 4.0. Server on Windows NT Server 3.51 and 4.0
Availbility: Shipping
Form completed by: Peter Ericson
Affiliation: Microsoft AB
Phone: +46 8 752 56 00
Fax: +46 8 750 51 58
Address: Finlandsgatan 30
164 93 KISTA

NetGain
Name of product: NetGain Mimetic
Version: 2.0
Manufactured by: NetGain
Tested on platform(s): Microsoft NT 3.51
Available on platform(s): Microsoft NT 3.51
Availablility: Now
Comments: For MS-Mail, cc:Mail and MEMO
Form completed by: Conny Jonsson
Email: conny.jonsson@netgain.se
Phone: +46-54-144450
Fax: +46-54-217980
Address: P.O. Box 289
651 07 Karlstad
Sales contact: Niklas Hellberg
Email: niklas.hellberg@netgain.se
Phone: +46-54-144450
Fax: +46-54-217980

Address: P.O. Box 289
651 07 Karlstad

Sun Microsystems AB
Name of product: Solstice Internet Mail client 0.9
Version: 0.9
Manufactured by: SunSoft
Tested on platform(s): SS-20, Solaris 2.5 CDE 1.0.1
Available on platform(s): Solaris 2.4-, and Windows
Availablility: Announced April -96 together with the imap-server
Comments: Earlier known as Roam (Snus tests -95)
Form completed by: Bertil Lindblad
Affiliation: Sun Microsystems AB, Stockholm (Kista)
Email: bertil.lindblad@sun.se
Phone: +46-8-623 92 16
Fax: +46-8-623 90 05
Address: Box 51
S-164 94 KISTA
Sales contact: Anders Arlberg
Affiliation: Marknadsavdelningen, Sun Stockholm
Email: anders.arlberg@sun.se
Phone: +46-8-623 90 00
Fax: +46-8-623 90 05

Sun Microsystems AB
Name of product: Pronto E-mail, part of PC-NFS pro 2.0
Version: 2.0.1
Manufactured by: SunSoft licensed from CommTouch SW, Inc
Tested on platform(s): Dell PC med Windows 3.11
Available on platform(s): Windows 3.x
Availablility: Now
Form completed by: Bertil Lindblad
Techincal reference: Ingvar Johansson
Affiliation: Sun Microsystems AB, Stockholm (Kista)
Email: bertil.lindblad@sun.se (ingvar.johanssson@sun.se)
Phone: +46-8-623 92 16 (623 92 38)
Fax: +46-8-623 90 05
Address: Box 51
S-164 94 KISTA
Sales contact: Anders Arlberg
Affiliation: Marknadsavdelningen, Sun Stockholm
Email: anders.arlberg@sun.se
Phone: +46-8-623 90 00
Fax: +46-8-623 90 05

TeamWARE Group
Name of product: TeamWARE Internet Mail V5
Version: V5
Manufactured by: TeamWARE Group
Tested on platform(s): Sun Solaris 2.5
Available on platform(s): Solaris, NT
Availablility: Solaris (5/96), NT (7/96)
Form completed by: Pentti Soini
Email: pentti.soini@icl.fi
Phone: +358-0-5696545
Fax: +358-0-5696498
Address: P.O.Box 780
00101 Helsinki
Finland
Sales contact: TeamWARE Group
Email: hotline.teamware@teamw.com
Phone: +358-0-5696767
Fax: +358-0-5656872
Address: P.O.Box 780
00101 Helsinki
Finland

Tele2
Name of product: ADMD InterX X.400-to-Internet Gateway
Comments: This is a platform for gatewaying MIME compliant e-mails to and from the X.400 enviroment.
Form completed by: Helena Svensson
Affiliation: Tele2
Email: helena.svensson@x400.swip.net
Phone: +46-8-5626 40 00
Fax: +46-8-5625 42 00
Address: Tele2 AB Box 62 164 94 Kista
Sales contact: Ordinary Tele2 Sales channels
Affiliation: Tele2
Email: info@swip.net
Phone: +46-8-5626 40 40
+46-31-720 59 50
+46-40-600 50 00
Fax: +46-8-5626 42 00
Address: Tele2 AB
Box 62
164 94 Kista

3 Test Summary

The tests are divided into 4 classes.

M - Minimal RFC-822 and MIME conformance, as described in relevant RFCs above.

SM - MIME and features which are necessary to communicate using Swedish language, i.e., extensions to the minimal conformance test to include handling of Swedish national characters in a uniform way.

EM - Extra MIME functionality such as handling of character sets not mentioned in class M or SM, and handling of other types of data, e.g., picures and sound. The results of these tests are not relevant for the certification process.

N - Non-MIME functionality, such as requirements on transfer systems and gateways.

EN - Extra non-MIME functionality, such as use of optional parameters in transfer systems. The results of these tests are not relevant for the certification process.
Programs that pass all tests in class M, SM, and applicable parts of N, will be certified as mail products suitable for use in Sweden.

3.1 Test Specification

The tests will primarily be carried out before the Interoperability Fair, by the participating parties. There will be a mailback server which will generate test messages with MIME content according to the specification, to test software capabilies for incoming mail. To test capabiliteies for outgoing mail, there will be a mailbox that is manually examined by the test leaders.

The participants are expected to complete a test form (Appendix A) with correct information regarding their software. The test forms are to be sent (as e-mail) to the test leaders no later than April 25, 1996. The test forms will be compiled into a preliminary document which will be handed out to Interop guests and visitors. During the actual Interoperability Fair, the test leaders will verify various sections of various test forms. The final results will be compiled and made part of the final Interoperability test report.

Test forms that are submitted later than the date above will neither be included in the preliminary, nor in the final test report.

Software participating in the test is supposed to be "as is", which means that it should be installed out of the box, with no special amendments from the participating organisation. All extra configuration, beyond normal setup expected by the user and according to the installation manual, is to be indicated in the test form as verbose comments. If the software requires external software to perform one or more tests, that should be clearly indicated, and a note should make clear whether that external software is included in the distribution of the tested software or not.

3.2 Reception Tests

To test if a client can parse a MIME message of a specific type, a mailback service is available, from which messages can be ordered. For more information, send a message to mimeback@bunyip.com with the command HELP as the only word in the subject line, e.g.,

To: mimeback@bunyip.com
Subject: HELP

You will receive a plain text messgage containing further instructions on how to use the mimeback server.

3.3 Transmission Tests

In many cases the participants are also expected to produce messages. To have an outgoing message verified, please send it to

mime-test@cafax.se

and not to any personal mailbox. A test leader will reply to the message with comments on its contents. Please make sure that the sender addresses of your test messages are valid return addresses.

3.4 Interoperability Tests

A mailing list

mime-participants@cafax.se

will be created to facilitate communication and cross-platform tests between the participants. This way it will be easy for participants to test the interopability of their software with other participants. Of course this course of action depends a lot on the good will and positive attitude of the participants. (Read: Don't abuse!)

3.5 Test responses

The result of each test can be either a clear "Yes", a "No", or a combination of "Not applicable" and a comment. One example is the tests about recieving SMTP connections, which are unapplicable for POP and IMAP clients. A "Yes" or a "No" may be accompanied by a comment giving extra information.

Tests regarding software's ability to handle MIME message types are to be interpreted as whether the software is able to handle it or not in its basic configuration.
If the user has to take extra measures to obtain the functionality it is to be indicated as "No" with an explaining comment starting with the expression "User configurable".

3.6 Test Criteria

The following are the test criteria that the software has to meet, to get certified in the indicated test class.

Class M - Minimal MIME conformance tests

M1 Always generate a "MIME-Version: 1.0" header field.

M2 Recognize the Content-Transfer-Encoding header field, and decode all received data encoded with either the quoted-printable or base64 implementations. Encode any data sent that is not in seven-bit mail-ready representation using one of these transformations and include the appropriate Content-Transfer-Encoding header field, unless the underlying transport mechanism supports non-seven-bit data, as SMTP does not.

(Interoperability comment: For clarification it is stated that software should implement both encodings, and be able to handle mail encoded in any one of them.)

M3 Recognize and interpret the Content-Type header field, and avoid showing users raw data with a Content-Type field other than text. Be able to send at least text/plain messages, with the character set specified as a parameter if it is not US-ASCII.

M4 Explicitly handle the following Content-Type values, to at least the following extents:

M4.1 Text

M4.1.1 Recognize and display "text" mail with the character set"US-ASCII."

M4.1.2 Recognize other character sets at least to the extent of being able to inform the user about what character set the message uses.

M4.1.3 Recognize the "ISO-8859-*" character sets to the extent of being able to display those characters that are common to ISO-8859-* and US-ASCII, namely all characters represented by octet values 0-127.

(Interoperability comment: Which glyphs to display for octets with values in the range 128-255 is up to the implementation.)

M4.1.4 For unrecognized subtypes, show or offer to show the user the "raw" version of the data after conversion of the content from canonical form to local form.

M4.2 Message

M4.2.1 Recognize and display at least the primary (822) encapsulation.

(Interoperability comment: Note that 822 is just a name of the subtype. See RFC-1521 for description of the type.)

M4.3 Multipart

M4.3.1 Recognize the primary (mixed) subtype. Display all relevant information on the message level and the body part header level and then display or offer to display each of the body parts individually.

M4.3.2 Recognize the "alternative" subtype, and avoid showing the user redundant parts of multipart/alternative mail.

M4.3.3 Treat all unrecognized subtypes as if they were "mixed".

M4.4 Application

M4.4.1 Offer to remove the Content-Transfer-Encoding. The software should be able to handle types of Content-Transfer-Encoding defined in RFC-1521. The resulting information should be written to a user file.

M5 Upon encountering any unrecognized Content-Type, treat the message as if it had a Content-Type of "application/octet-stream" with no parameter subarguments. How such data are handled is up to an implementation, but suggested options for handling such unrecognized data include offering the user to write it to a file (decoded from its mail transport format) and offering the user to name a program to which the decoded data should be passed as input. Unrecognized predefined types, which might include audio, image, or video, should also be treated in this way.

Class S - Minimal functionality required in Sweden

S1 Ability to send and receive text/plain message types according to rule M4.1.1 with the extension that in character set ISO-8859-1 the octets values 128-255 (decimal) must be displayed using the correct glyphs.

(Interoperability comment: It is acceptable that some graphic symbols are not displayed correctly if the reason for that is that no complete translation table between ISO-8859-1 and the native character set can be generated.)

S2 Ability to send and receive messages with header lines encoded according to RFC-1522 with character set ISO-8859-1. Recognize other "ISO-8859-*" character sets to the extent of being able to display those characters that are common to ISO-8859-* and US-ASCII, namely all characters represented by octet values 0-127.

Class EM - Extra tests about MIME functionality
Tests of specific MIME types. For each type, it should be noted if the content type can be received and/or sent with the software unsing the basic

configuration installed out of the box. If the content type can be recieved/sent, but only after additional configuration, that must be clearly stated in the test form. If the content type is displayed/composed by using external software, that must also be clearly stated.

EM1 Content-Type Text

Is the software able to handle messages with the following specifications.

EM1.1 Charset Parameters to Type Text/Plain

EM1.1.1 text/plain; charset=SEN_850200_B

EM1.1.2 text/plain; charset=ISO-2022-JP-2

EM1.2 text/enriched

EM2 Content-Type Image

EM2.1 image/gif

EM2.2 image/jpeg

EM2.3 image/tiff

EM3 Content-Type Audio

EM3.1 audio/basic

EM4 Content-Type Application

EM4.1 application/msword

EM4.2 application/postscript

EM5 Content-Type Multipart

EM5.1 multipart/appledouble

EM5.2 multipart/report

This format is specified in Internet-Drafts created by the IETF Notary Working Group. For gateways from/to X.400, the definitions can be found in Internet drafts created by the IETF Mixer Working Group.

EM6 Content-Type Message

EM6.1 message/partial

EM6.2 message/external-body (This test uses multipart/alternative also). It must be noted which access types are supported.

EM7 Content-Type Video

EM7.1 video/mpeg

EM7.2 video/quicktime

Class N - Extra tests about non-MIME functionality

The following requirements are not related to MIME message content specifications, but must be met to receive full SNUS certification.

N1 The date used must follow recommendations in RFC-1123. (Interoperability comment: One example: the time-zone must be numerical in the form +NNNN or -NNNN.)

N2 SMTP Servers

N2.1 When acting as SMTP server, the program must be "stable", i e, it must accept lines longer than 80 characters, accept unknown tokens, accept known tokens in wrong order etc, without disconnecting the client. Sensible error messages should be generated.

N2.2 An SMTP server must honour the RSET command at any time when a command is to be expected in the dialog.

N2.3 An SMTP server must be able to handle multiple (more than 3) simultanous TCP-connections and carry out a dialog on each of them.

N2.4 An SMTP server must act sensibly upon receipt of mail not addressed to a domain it represents. Either the message should be rejected (with a sensible error code in the 500 series) in the SMTP dialog, or it should be bounced correctly to the envelope sender, or it whould be forwarded properly in the direction indicated by the envelope address(es).

N3 SMTP Clients

N3.1 An SMTP client must be able to handle multiple line messages from the server in any situation where a message from the server is to be expected. This also concerns the initial greeting message from the server.

N3.2 An SMTP client must never send high octets (i.e., with values in the range 128-255) without first having verified that the server is able to handle them. One method of such verification is the 8BITMIME STMP extension. Note that headerlines never may contain high octets. Header lines must be encoded according to RFC-1522.

The client must never use high octets in envelope addresses.

Class EN

The following tests reflect extra functionality without connectin to MIME message content specifications. The tests should be completed, but the outcome is not relevant for SNUS certification.

EN1 Attachments in non-MIME format

EN1.1 Attachment is recognized if the encoding is uuencode, i.e., one line in the message is:

begin 666 filename

EN1.2 Attachment is recognized if the encoding is BinHex4.0, i.e., one line in the message is:

(This file must be converted with BinHex4.0)

EN2 SMTP servers - ESMTP and DNS

EN2.1 The server recognizes the EHLO command and reacts accordingly by listing its extensions.

EN2.2 The server handles the SIZE extension. (RFC-1653)

EN2.3 The server handles the 8BITMIME extension correctly. This implies that the server is able to convert the content-transport-encoding if required in the next hop. (RFC-1652)

EN2.4 The server handles the DSN extension correctly. (RFC-1891 and RFC-1894).

EN3 SMTP clients - ESMTP and DNS

EN3.1 The client uses EHLO to determin if the server in question is able to handle SMTP extensions.

EN3.2 The client recognizes and uses the SIZE extension correctly. (RFC-1653)

EN3.3 The client recognizes and uses the 8BITMIME extension correctly. (RFC-1652)

EN3.4 The client is able to recognize and use the DSN extension correctly. (RFC-1891 and RFC-1894).

EN3.5 The client is able to use the DNS system and its MX records to determin which SMTP server to contact, determined by the recipient envelope address(es).

4 The results

The results are basically Y or N. If there is a comment on the result (a footnote) that is most of the time negative if it is on a Y and positive if it is on an N. The Y can be followed by an I to describe that the functionality tested is handled internally in the software, or an E to show that its is handled in an external module.

NA means that that test is not applicable to this software.

A '–' shows that the test result was either missing from the report or so unclear that it seems that the testing person was confused by our test specification or something else which makes the result unusable in this report.

Results:

	1	2	3	4	5	6	7	8	9	10
M1	Y	Y	Y	NA	Y	Y	Y	Y	Y	Y
M2	Y	Y	Y	NA2	Y	Y	N3	Y	Y	Y
M3	Y	Y	Y	NA	Y	Y	Y	Y	Y	Y
M4.1.1	Y	Y	Y	NA	Y	Y	Y	Y	Y	Y
M4.1.2	Y	Y	Y	NA	Y	Y	Y	Y	Y	Y
M4.1.3	Y4	Y5	Y	NA	Y6	Y7	Y	Y	Y8	Y
M4.1.4	Y	NA	Y	NA	Y	Y	Y	Y	Y	Y
M4.2.1	Y	–	Y	NA	Y	Y	Y	Y	Y	Y
M4.3.1	Y	–	Y	NA	Y	Y	Y	Y	Y	Y
M4.3.2	Y	–	Y	NA	Y9	Y	Y	Y	Y	Y
M4.3.3	Y	Y	Y	NA	Y	Y	Y	Y	Y	Y
M4.4.1	Y	N	Y	NA	Y	Y	Y	Y	Y	Y
M5	Y10	–	Y	NA	Y	Y	Y	Y	Y	Y
S1	Y11	Y12	Y	NA	Y	Y	Y	Y	Y	Y
S2	Y13	Y14	Y15	NA	Y16	Y17	N	Y18	Y19	Y
EM1.1.1	YI	YI	YI	NA	YI	Y	N	N	N	Y
EM1.1.2	N	N	YE	NA	N20	YE	N	N	N	NA
EM1.2	N	–	YE	NA	N	N	N	N	N	Y
EM2.1	YE	–	YE	NA	YE	YE	YE	YE	Y	Y
EM2.2	YE	–	YE	NA	YE21	YE	YE	YE	Y	Y
EM2.3	YE	–	YE	NA	YE22	YE	YE	N	N	Y
EM3.1	YE	–	YE	NA	N	YE	–	YE	Y	Y
EM4.1	YI	–	YE	NA	YE	YE	–	–	N	Y
EM4.2	YE	–	YE	NA	N	YE	–	YE	Y	Y
EM5.1	N23	–	N24	NA	N	N25	N26	N27	N	Y
EM5.2	–	–	Y28	NA	N	Y29	–	–	N	Y
EM6.1	–	–	N	NA	N	Y	N	N	Y	Y
EM6.2	Y30	–	Y31	NA	N	N32	N	Y	Y	N
EM7.1	–	–	YE	NA	N	YE	–	N	Y	Y
EM7.2	–	–	YE	NA	N	YE	–	N	N	Y
N1	–	–	Y	Y33	Y	Y	–	–	Y	Y
N2.1	–	–	NA	Y	Y	Y	–	–	Y	Y

N2.2	-	-	NA	Y	Y	Y	-	-	Y	Y
N2.3	-	-	NA	Y	Y	Y	-	-	Y	Y
N2.4	-	-	NA	Y	Y	Y	-	-	Y	Y
N3.1	-	-	Y	Y	N	Y	-	-	Y	Y
N3.2	-	-	Y	Y	-	Y	-	-	Y	NA
EN1.1	-	-	Y	NA	Y	Y	-	-	N	N
EN1.2	-	-	N	NA	N	N	-	-	N	N
EN2.1	-	-	NA	Y	N34	Y	-	-	N	Y
EN2.2	-	-	NA	Y	-	N	-	-	N	Y
EN2.3	-	-	NA	Y35	-	Y	-	-	N	N
EN2.4	-	-	NA	N	N	N	-	-	N	N
EN3.1	-	-	Y	Y	N	Y	-	-	N	Y
EN3.2	-	-	N	Y	N	N	-	-	N	Y
EN3.3	-	-	Y	Y	N	Y	-	-	N	N
EN3.4	-	-	N	N	N	N	-	-	N	N
EN3.5	-	-	N	Y	Y36	Y	-	-	N	N

5 General comments:

DES Communication

Unfortunately, the test report that DES communication handled in was only the result after using the MIME mailback server handled by the SNUS test team. No information from how the SMTP MTA worked were available or reported in the test report, and because of that the result for the MTA (which is the kind of software this software is) is unknown. The results reported are for the user agent Microsoft Exchange 4.0, which is not part of the package from DES communications. Because of this, and the fact that that the tests that have to do with the MTA, the tests of how ESMTP is handled, was not done, a descision of if this software passes the SNUS MIME tests can not be done at this stage.

GE Information Services

Many results from the tests are missing, which makes the descision if this software can pass the SNUS MIME tests impossible to make.

ICL

EMBLA is an IMAP/POP client for Windows (95, 3.1*, NT) which have no problem passing all required tests.

Matti Aarnio

Zmailer is an MTA which is an alternative to the othervise so popular Sendmail. It handles all necessary MIME and ESMTP things (like 8BITMIME and DSN receipts).

The evolution of new functionality is always going on for "exclusive" features like 8BITMIME support for non text/plain messages. Even though these tests are constructed for email clients, we accepted Zmailer as a software package to test and can not say more than it passes our requirements.

Microsoft AB

The Exchange package have both clients and servers which handles MIME well. Old bugs in the MIME and email handling system is over time removed from the software, and this is a package which passes all tests for MIME software. Some exclusive features are of course missing still, but that is the case for all software.

NetGain

NetGain Mimetic is a gateway between SMTP and one of MS-Mail, CC:Mail or MEMO. The functionality is good and it passes all requirements both on the MTA requirements and the MIME capabilites needed for gatwaying messages.

Sun Microsystems (Pronto)

Pronto is an email client for Windows that which do not have all the functionality needed for use in Sweden. It can for example not encode/decode header lines according to RFC 1522.

Sun Microsystems (Solstice)

The Solstice client is previously known as ROAM and is getting closer and closer to being a real MIME client. As it is today, it seems that some basic configuration is needed to handle attachments. No "interesting" attachments can be handled automatically. BUT, it can handle all necessary MIME stuff for use in Sweden.

TeamWare

The TeamWare Internet Mail is a software package that participated for the first time this year. The functionality is good, but note that it was not reported if the viewers needed for some MIME types was not reported if they were "Internal" or "External" viewers. The TeamWare software passes the MIME tests this year.

Tele2

The gateway to/from X.400 run by Tele2 fulfils all criteria that can be applied to a gateway to/from SMTP. As a general comment from Tele2, most tested body parts are only tested from SMTP to X.400 and not in the other direction because they can not be generated in X.400.

Comments to the result table:

---

1. Tested with Microsoft Exchange Client version 4.0. Borderware Firewall server is an MTA only.
2. Will encode in Quoted Printable when necessary.
3. Handles Quoted-Printable, but not Base64.
4. Unclear how characters in the range 128-255 are handled.
5. Unclear what glyphs are used for chacters in the range 128-255.
6. Unclear what glyphs are used for chacters in the range 128-255.
7. Characters missing in the target character set is replaced by special character.
8. Unclear what glyphs are used for chacters in the range 128-255.
9. Only one part is displayed to the user, but the user have to pick which one himself.
10. Unclear how unrecognized subtypes are handled.
11. Unclear how all characters in the range 160-254 are handled.
12. How all characters in the range 160-254 are handled are unknown.
13. Unclear how characters in the character sets ISO-8859-2 to ISO-8859-10 are handled.
14. How characterset ISO-8859-2 to ISO-8859-10 are handled are unknown.
15. How character set ISO-8859-2 to ISO-8859-10 are handled are unclear.
16. How character set ISO-8859-2 to ISO-8859-10 are handled are unclear.
17. How character set ISO-8859-2 to ISO-8859-10 are handled are unclear.
18. How character set ISO-8859-2 to ISO-8859-10 are handled are unclear.
19. How character set ISO-8859-2 to ISO-8859-10 are handled are unclear.
20. Only available in Japanese version.
21. The external viewer is not included in the distribution.
22. The viewer is not part of the distribution.
23. Can handle these with external viewer after reconfiguration of client.
24. Treated as multipart/mixed.
25. Treated as multipart/mixed.
26. Treated as multipart/mixed.
27. Treated as multipart/mixed.
28. Treated as a new message.
29. Treated as a new message.
30. Results are unclear.
31. Unclear what access types are supported.
32. The software informs about how the message can be obtained.
33. Applies only to date/time stamps generated by this mailer, not to those fed to it via some submission method.
34. Will be available in maintanance release after the summer.
35. Only for text/plain messages.
36. The server side is using MX records.

3:3 ATM LAN-EMULERING
ATM LAN-EMULATION

Testledare/Testmanager:
Niklas Gerdin, Frontec

Sidor/*Pages:*
16

Deltagare/Participants:	*Produkt/Product*
Lennart Preuss	AU-system
Olle Åslund	Bay Networks
Niklas Montin	Cisco Systems
Christer Dierks	Telia Systems (Swedish Telecom)
Johan Ekelundh	Sun Microsystems
Rolf Börjeson	3Com
Jan Munkhammar	UB Networks

ATM LAN Emulation Testreport and Testspecification

1 Testleader

Niklas Gerdin — Frontec Network Services AB <Niklas.Gerdin@sth.frontec.se>
(Northern Telecom B.V , Holland after the 1 of November 1996)

2 Participants

Lennart Preuss	Au-System	<lps@ausys.se>
Olle Åslund	Bay Networks	<oaslund@baynetworks.com>
Niclas Montin	Cisco Systems	<nmontin@cisco.com>
Chister Dierks	Telia Systems (Swedish Telecom)	<christer.e.dierks@telia.se>
Johan Ekelundh	Sun Microsystems	<Johan.Ekelundh@sun.se>
Rolf Börjeson	3Com	<Rolf_Borjesson@3Com.com>
Jan Munkhammar	UB Networks	<jmunkham@ub.com>

3 Test Summary

The tests were conducted in april 1996.

The 1996 version of ATM LAN emulation tests the basic functions of ATM LAN Emulation LECS, LES, LEC and BUS. We will test the connectivity between different ATM LAN Emulation vendors in an ATM network. The previous ATM LAN emulation test 1995 did not meet their goals, why this is an important test to prove correct functions of ATM LAN emulation in a mixed ATM LAN emulation network environment.

4 Goals and Objectives ATM LAN Emulation

The objectives with ATM LAN emulation tests are to give the datakommunicationsspecialists the ability to test ATM LAN emulation products from different companies against their own products. The goals are to receive knowledge about different implementations of ATM LAN emulation. The reader of the testreport should be able to receive the information he or she need before the investment in ATM LAN emulation equipment.

5 Description of ATM LAN emulation (ATM LANE)

LAN Emulation as the name tells is an emulated LAN in an ATM network. ATM LAN emulation defines the service interface against a higher OSI layer. That is the network layer protocol. This protocol is identical towards the current LAN standards like IEEE 802.3 and IEEE 802.5. The two IEEE protocols can operate over an ATM network via the ATM LAN emulation protocol. ATM LAN emulation is not trying to emulate the actual media access protocol attach to an ATM network. The basic function of ATM LAN emulation protocol is to resolve MAC addresses into ATM addresses. It is a protocol for MAC bridging (switching) over an ATM network. ATM LAN emulation uses the same drivers as existing MAC protocols. It means no changes of the higher level protocol in order to operate within an ATM network. We can have more than one VLAN within an ATM network.

6 History (Mikael Lundblad ATM LAN Emulation tests 1995)

The testleader in Interoperabilitet-95 Mikael Lundblad has commented ATM LAN Emulation 1995 tests in the following words. "The ATM-UNI 3.0 signalling SVC works fine between Cisco and Digital, congratulations ". The InATMARP request from the DEC-station was not responded to by the Cisco router. Support for this is required by RFC1577. Futher examinations with Cisco show that they have partly implemented RFC1577. Cisco supports only static ARP-entries in the tested release and Digital has requirements for InATMARP." The testresult was "no functionality achieved" between the equipment tested.

7 Test Procedure ATM LAN Emulation 1996

The LAN Emulation tests the interoperability of LECS, LES, LEC and BUS between different vendors of ATM switches. It tests also interoperability between different vendors.

8 Test purpose

The purpose of ATM LAN Emulation is to verify correct functions of UNI 3.0/3.1, ILMI, SVC, point-multipoint and ATM LANE Phase 1. The goal is to test interoperability between vendors of ATM LANE services.

9 Hardware and Software

Participants Au-System
Vendor ForeSystem

Products

FORESYSTEMS	SOFTWARE	ATM FUNCTION
Forerunner ES-3810	4.0.0_1.7	ATM LANE LEC
Forerunner ASX-200WG	4.0.0_1.35	ATM Switch ATM LANE LECS, LES, BUS
Forerunner PC card PCA-200E	4.0.0_1.37	ATM LANE LEC

Participants Cisco Systems
Vendor Cisco Systems

Products

CISCO SYSTEMS	SOFTWARE	ATM FUNCTION
Catalyst 5000	1.5/2.1	ATM LANE LES, LECS, BUS, LEC
Cisco 7010	11.0(7)	ATM LANE LES, LECS, BUS, LEC
Cisco LS100	3.1(1)	ATM Switch LECS to the LEC's via ILMI
Cisco LS 1010	11.0(90.43)	ATM Switch LECS to the LEC's via ILMI

Participants Sun Microsystems
Vendor Sun Microsystems

Products

SUN MICROSYSTEMS	SOFTWARE	ATM FUNCTION
Sun ATM 1.0 SBus-Card	2.0	ATM LANE LEC

Participants 3Com
Vendor 3Com

Products

3COM	SOFTWARE	ATM FUNCTION
Cellplex 7000	3.0	ATM Switch ATM LANE LECS, LES, BUS
Linkswitch 2700	3.0	ATM LANE LEC

Participants UB Networks
Vendor UB Networks

Products

HARDWARE	SOFTWARE	ATM FUNCTION
GeoSwitch	1.3.4	ATM Switch ATM LANE LECS, LES, BUS
Interphase 4615 ATM Sbus Adapter	SJ00049-A.01	ATM LANE LEC

Participants Telia Systems (Swedish Telecom)
Vendor First Virtual

Products

FIRSTVIRTUAL	SOFTWARE	ATM FUNCTION
FSW1000	LANE 3.00K, SW 3.00X	ATM Switch ATM LANE LECS, LES, BUS
FVC ISA+	3.00B	ATM LANE LEC

Participants BayNetworks
Vendor BayNetworks

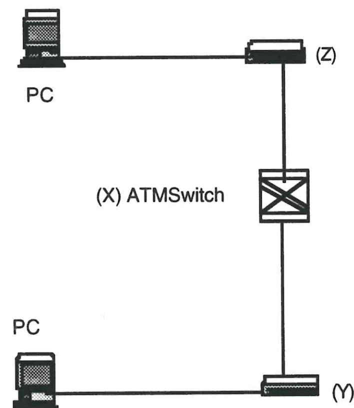
Products

BAYNETWORKS	SOFTWARE	ATM FUNCTION
5000AH	2.01	ATM LANE LECS, LES, BUS
Ethercell 10328-F	2.01	ATM LANE LEC
Wellfleet BLN VNR	10.0 4	ATM LANE LEC

10 Test specification and procedures

10.1 Step 1, Two and two tests with different vendors

X and Y is two separated vendors that should test against each other. X is setting up an ATMswitch within an ATM network. The vendor X is offering LECS, LES and BUS services to the clients. The Clients Y (LEC) and Z (LEC) can work as an ATMaccess product, IEEE 802.3 LAN card or via an Ethernet (TokenRing) router.



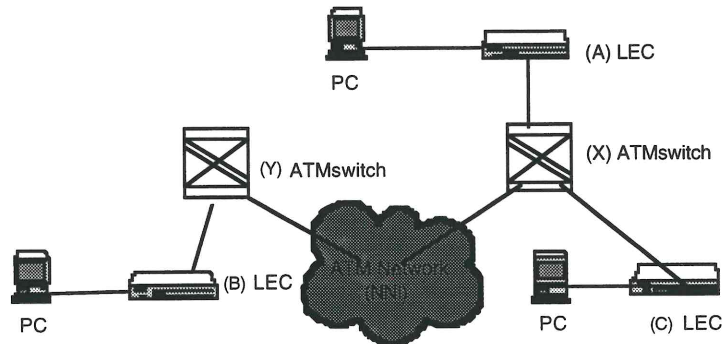
The test purpose is to establish contact between Y and the LECS, BUS, LES services in the ATMswitch. This gives us the opportunity to check, which VLAN Y is connecting. We will receive the LES and BUS services for our VLAN. The next part of the test is to establish contact with the other point Z.

10.2 Step 2, Switch the vendor of the ATMswitch

Y and X will switch location and follow the procedure as step 1 describes.

10.3 Step 2+, Double ATMswitches

Both X and Y are setting up ATMswitches in the ATM network. The two ATMswitches connect via IISP protocol or wellknown ATM address. The X and Y accessproducts test against the ATM network.



10.4 Step 3, More accessproducts

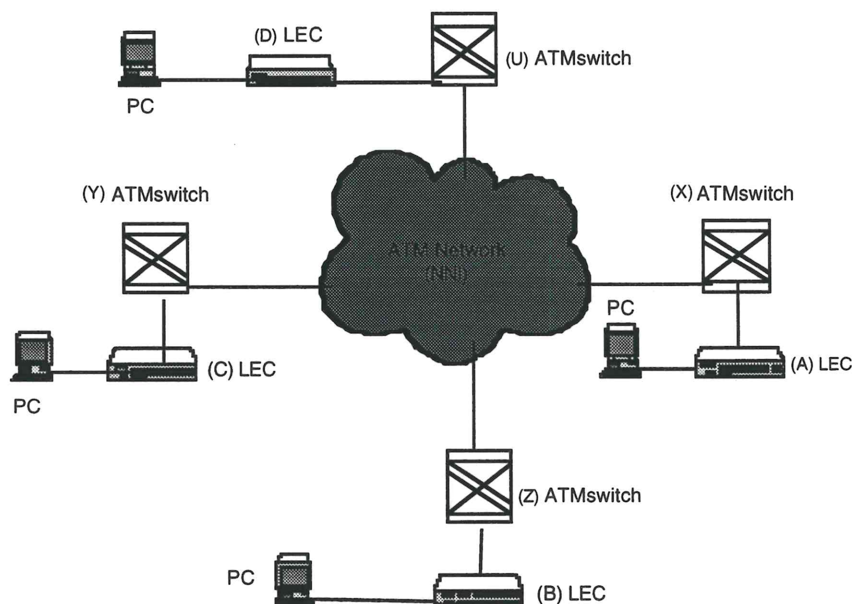
X has an ATMswitch in the ATMnetwork, and more accessproducts vendor connects via A, B, C,etc.

10.5 Step 4 Switch ATMswitch vendor

Y is setting up an ATMswitch and the rest of the access products is in the test. The test repeats as in step 1 and 3.

10.6 Step 4+ More ATMswitches

This will be an multi-switched ATM network. The network has many different ATMswitches connected with the UNI to NNI (IISP) protocol or Wellknown ATM address.



11 Testresults step 1 and 2

11.1 Cisco Catalyst 5000 ATM LANE services LECS, LES and BUS



ATM LANE CLIENT LEC	FUNCTIONALITY AND CONNECTIVITY (PING AND CORRECT ADDRESS TABLES)
Cisco 7010 ATM LANE Card	OK
3Com Linkswitch 2700	OK
Forerunner PCA-200E (PCI-Card)	OK
Foreunner ES-3810	OK
Interphase ATM Sbus-Card	* No OK
Sun ATM Sbus-Card 1.0	OK
FVC ISA+	OK
BayNetworks Ethercell 10328-F	** No OK
Wellfleet BLN VNR	*** No OK

Comments

All Connections established with the ATM well-known address.

* Interphase ATM SBus card is requesting an MTU size less than 1516 bytes. The specification identicate an MTU size of 1516 bytes for ATM LAN Emulation.

* * The ATM LANE network was not stabile. The "ping" command did work. The products joined and left the ATM LAN emulation network all the time during the test. It looked like a timing problem.

*** We suspected problems with the ILMI between the two products.

11.2 Cisco 7010 ATM LANE services LECS, LES, LEC and BUS



ATM LANE CLIENT LEC	FUNCTIONALITY AND CONNECTIVITY (PING AND CORRECT ADDRESS TABLES)
Wellfleet BLN VNR	*** No OK
3Com Linkswitch 2700	OK
Forerunner PCA-200E (PCI-Card)	OK
Foreunner ES-3810	OK
Interphase ATM Sbus-Card	* No OK
Sun ATM Sbus-Card 1.0	OK
FVC ISA+	OK
Cisco Catalyst 5000 ATM LANE Card	OK
BayNetworks Ethercell 10328-F	** No OK

Comments

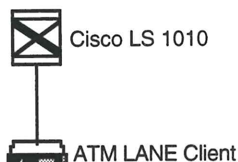
All Connections established with the ATM well-known address.

* Interphase ATM SBus card is requesting an MTU size less than 1516 bytes. The specification identicate an MTU size of 1516 bytes for ATM LAN Emulation.

* * The ATM LANE network was not stabile. The "ping" command did work. The products joined and left the ATM LAN emulation network all the time during the test. It looked like a timing problem.

*** We suspected problems with the ILMI between the two products.

11.3 Cisco LightStream 1010 ATM LANE services ILMI/UNI and IISP (LECS)



ATM LANE CLIENT LEC	FUNCTIONALITY AND CONNECTIVITY (PING AND CORRECT ADDRESS TABLES)
Cisco 7010	OK
3Com Linkswitch 2700	OK
Forerunner PCA-200E (PCI-Card)	OK
Foreunner ES-3810	OK
Interphase ATM Sbus-Card	* No OK
Sun ATM Sbus-Card 1.0	** No Test
FVC ISA+	OK
Cisco Catalyst 5000	OK
BayNetworks Ethercell 10328-F	*** No Test
Wellfleet BLN VNR	*** No Test

Comments

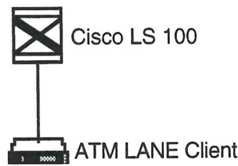
All Connections established with the ATM well-known address.

* Interphase ATM SBus card is requesting an MTU size less than 1516 bytes. The specification identicate an MTU size of 1516 bytes for ATM LAN Emulation.

** Not attending the test or no time to test the equipment

*** BayNetworks did not attend in the final tests due to unreleased software.

11.4 Cisco LS100 ATM LANE services ILMI/UNI and IISP (LECS)



ATM LANE CLIENT LEC	FUNCTIONALITY AND CONNECTIVITY (PING AND CORRECT ADDRESS TABLES)
Cisco 7010	OK
3Com Linkswitch 2700	OK
Forerunner PCA-200E (PCI-Card)	OK
Foreunner ES-3810	OK
Interphase ATM Sbus-Card	* No OK
Sun ATM Sbus-Card 1.0	OK
FVC ISA+	OK
Cisco Catalyst 5000	OK
BayNetworks Ethercell 10328-F	** No OK
Wellfleet BLN VNR	*** No OK

Comments

All Connections established with the ATM well-known address.

* Interphase ATM SBus card is requesting an MTU size less than 1516 bytes. The specification identicate an MTU size of 1516 bytes for ATM LAN Emulation.

* * The ATM LANE network was not stabile. The "ping" command did work. The products joined and left the ATM LAN emulation network all the time during the test. It looked like a timing problem.

*** We suspected problems with the ILMI between the two products.

11.5 3Com Cellplex 7000 ATM LANE services LECS, LES and BUS



ATM LANE CLIENT LEC	FUNCTIONALITY AND CONNECTIVITY (PING AND CORRECT ADDRESS TABLES)
BayNetworks Ethercell 10328-F	OK
3Com Linkswitch 2700	OK
Forerunner PCA-200E (PCI-Card)	OK
Foreunner ES-3810	OK
Interphase ATM Sbus-Card	OK
Sun ATM Sbus-Card 1.0	OK
FVC ISA+	OK
Wellfleet BLN VNR	OK
Cisco 7010	OK
Cisco Catalyst 5000	OK

Comments

All Connections established with the ATM well-known address.

11.6 BayNetworks 5000 AH ATM LANE services LECS, LES and BUS



ATM LANE CLIENT LEC	FUNCTIONALITY AND CONNECTIVITY (PING AND CORRECT ADDRESS TABLES)
BayNetworks Ethercell 10328-F	OK
3Com Linkswitch 2700	OK
Forerunner PCA-200E (PCI-Card)	* No
Foreunner ES-3810	* No
Interphase ATM Sbus-Card	** No Test
Sun ATM Sbus-Card 1.0	** No Test
FVC ISA+	** No Test
Wellfleet BLN VNR	OK
Cisco Catalyst 5000	OK
Cisco 7010	OK

Comments

All Connections established with the ATM well-known address.
* BayNetworks needs a null string or numbers as domainname.
They will return the string "default" as number 1 to the corresponding LEC.
Foresystems can not have a null string or the number 1 as domainname. Cisco 7010, Cisco Catalyst 5000, Cisco LS100 and 3Com Linkswitch 2700 can have the number 1 as domainname.
BayNetworks and Foresystems will correct above problems in the next release of the software.
** Not attending the test or no time to test the equipment

11.7 Forerunner ES-3810 ATM LANE services LECS, LES, LEC and BUS

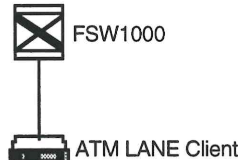


ATM LANE CLIENT LEC	FUNCTIONALITY AND CONNECTIVITY (PING AND CORRECT ADDRESS TABLES)
BayNetworks Ethercell 10328-F	OK
3Com Linkswitch 2700	OK
Forerunner PCA-200E (PCI-Card)	OK
Foreunner ES-3810	OK
Interphase ATM Sbus-Card	* No
Sun ATM Sbus-Card 1.0	OK
FVC ISA+	OK
Wellfleet BLN VNR	OK
Cisco 7010	OK
Cisco Catalyst 5000	OK

Comments

All Connections established with the ATM well-known address.
Interphase ATM SBus card is requesting an MTU size less than 1516 bytes. The specification identicate an MTU size of 1516 bytes for ATM LAN Emulation.

11.8 First Virtual FSW1000 ATM LANE services LECS, LES and BUS

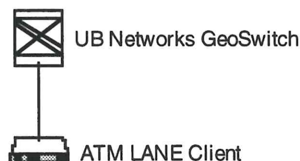


ATM LANE CLIENT LEC	FUNCTIONALITY AND CONNECTIVITY (PING AND CORRECT ADDRESS TABLES)
BayNetworks Ethercell 10328-F	* No Test
3Com Linkswitch 2700	OK
Forerunner PCA-200E (PCI-Card)	OK
Foreunner ES-3810	OK
Interphase ATM Sbus-Card	OK
Sun ATM Sbus-Card 1.0	OK
FVC ISA+	OK
Wellfleet BLN VNR	* No Test
Cisco 7010	OK
Cisco Catalyst 5000	OK

Comments

All Connections established with the ATM well-known address.
* BayNetworks did not attend in the final tests due to unreleased software.

11.9 UB Networks GeoSwitch ATM LANE services LECS, LES and BUS



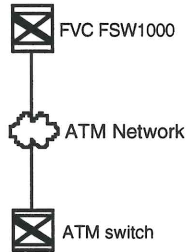
ATM LANE CLIENT LEC	FUNCTIONALITY AND CONNECTIVITY (PING AND CORRECT ADDRESS TABLES)
BayNetworks Ethercell 10328-F	* No Test
3Com Linkswitch 2700	OK
Forerunner PCA-200E (PCI-Card)	OK
Foreunner ES-3810	OK
Interphase ATM Sbus-Card	OK
Sun ATM Sbus-Card 1.0	OK
FVC ISA+	OK
Wellfleet BLN VNR	* No Test
Cisco 7010	OK
Cisco Catalyst 5000	OK

Comments

All Connections established with the ATM well-known address.
* BayNetworks did not attend in the final tests due to unreleased software.

12 Testresults step 2+ (Switch to Switch tests)

12.1 First Virtual FSW 1000 ATM Switch



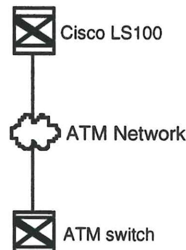
ATM SWITCHES	FUNCTIONALITY AND CONNECTIVITY (PING AND CORRECT ADDRESS TABLES)
Cisco LS100	OK
Cisco LS1010	OK
Forerunner ASX-200WG	OK
3Com Cellplex 7000	OK
UB Networks GeoSwitch	OK
First Virtual FSW1000	OK
BayNetworks 5000AH	* No Test

Comments

All Connections established with the ATM well-known address.

* BayNetworks did not attend in the final tests due to unreleased software.

12.2 Cisco LS100 ATM Switch

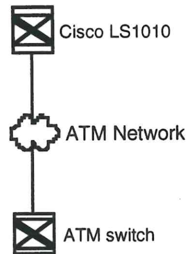


ATM SWITCHES	FUNCTIONALITY AND CONNECTIVITY (PING AND CORRECT ADDRESS TABLES)
Forerunner ASX-200WG	OK
3Com Cellplex 7000	* No OK
First Virtual FSW1000	OK
Cisco LS100	OK
UB Networks GeoSwitch	OK
BayNetworks 5000AH	** No OK

Comments

All Connections established with the ATM well-known address.
* See the testresults from on the LS1010 ATM Switch
** No testresult

12.3 Cisco LS1010 ATM Switch



ATM SWITCHES	**FUNCTIONALITY AND CONNECTIVITY (PING AND CORRECT ADDRESS TABLES)**
Forerunner ASX-200WG	OK
3Com Cellplex 7000	* No OK
First Virtual FSW1000	OK
Cisco LS100	OK
UB Networks GeoSwitch	** No OK
BayNetworks 5000AH	*** No Test

Comments

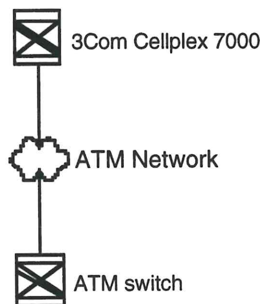
All Connections established with the ATM well-known address.

* The attendee needed more training with the products to justify a correctly set-up of the equipment corresponding against the Cisco equipment. 3Com and Cisco engineers experimented with time-out parameters to find a perfect match. The good guess is a configuration mismatch between both vendors. We could see problems with ATM signalling between 3Com and Cisco.

** No testresult

*** BayNetworks did not attend in the final tests due to unreleased software.

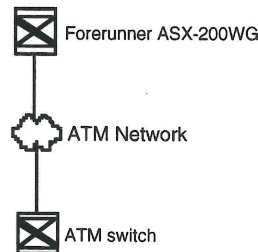
12.4 3Com Cellplex 7000 ATM Switch



ATM SWITCHES	FUNCTIONALITY AND CONNECTIVITY (PING AND CORRECT ADDRESS TABLES)
Forerunner ASX-200WG	* No OK
First Virtual FSW1000	* * OK
Cisco LS100	*** No OK
Cisco LS1010	*** No OK
UB Networks GeoSwitch	* No OK
BayNetworks 5000AH	**** No Test

Comments
All Connections established with the ATM well-known address.
* No Test result
* * The tests with "ping" shortly interrupts every minute. It seems like timing problem.
*** The attendee needed more training with the products to justify a correct set-up of the equipment corresponding against the Cisco equipment. 3Com and Cisco engineers experimented with time-out parameters to find a perfect match. The good guess is a configuration mismatch between both vendors. We could see problems with ATM signalling (flowcontrol) between 3Com and Cisco.
**** BayNetworks Networks did not attend in the final tests due to unreleased software.

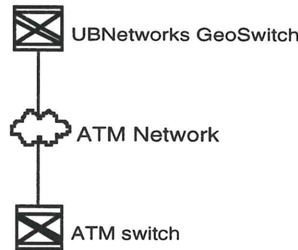
12.5 Forerunner ASX-200WG ATM Switch



ATM SWITCHES	FUNCTIONALITY AND CONNECTIVITY (PING AND CORRECT ADDRESS TABLES)
First Virtual FSW1000	OK
Cisco LS100	OK
Cisco LS1010	OK
UB Networks GeoSwitch	* No OK
3Com Cellplex 7000	** No OK
BayNetworks 5000AH	*** No Test

Comments
All Connections established with the ATM well-known address.
* No Testresult
** The attendee needed more training with the products to justify a correctly set-up of the equipment corresponding against the Foresystem equipment. The engineers experimented with time-out parameters to find a perfect match. The good guess is a configuration mismatch between both vendors. We could see problems with ATM signalling (flowcontrol) between 3Com and Foresystem.
*** BayNetworks did not attend in the final tests due to unreleased software.

12.6 UB Networks GeoSwitch ATM Switch



ATM SWITCHES	FUNCTIONALITY AND CONNECTIVITY (PING AND CORRECT ADDRESS TABLES)
First Virtual FSW1000	OK
Cisco LS100	OK
Cisco LS1010	OK
3Com Cellplex 7000	* No OK
BayNetworks 5000AH	** No Test
Forerunner ASX-200WG	* No Test

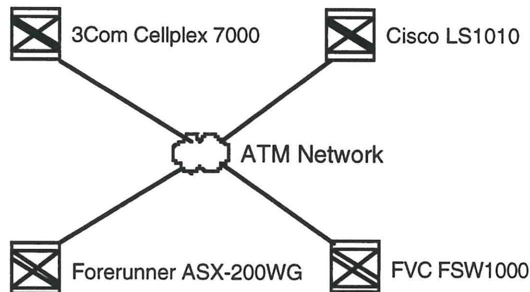
Comments

All Connections established with the ATM well-known address.

* No testresult

** BayNetworks did not attend in the final tests due to unreleased software.

13 Testresults step 4+ (multi-switched network)



We are testing all the qualified ATM switches with ATM LAN emulation services enabled with different domainnames. The domains are cisco (Cisco LS1010), coms (3Com Cellplex 7000), first (First Virtual FSW1000) and default (Forerunner ASX-200WG). We have one VLAN in every domain in the ATM network. The LES service in the different VLAN's is connecting different vendors ATM LAN emulation LEC's. We have several VLAN's in the ATM network.

Comments

We did have 2 switches with 3 vendor's clients connected running two VLANS with routing between them. The LECS in Cisco 7010, routing between VLANS in the Cisco 7010. The LES/BUS in the Cisco7010 and the Forunner ASX-200WG. The LES in the Cisco Catalyst 5000, the 3Com linkswitch 2700 and the Forerunner ES-3810. The "ping" command worked between the connected VLANS.

15 Summary ATM LAN Emulation test on the Interoperabilitet-96

The testleader sincerely thanks all the participants in the ATM LAN emulation tests. The conclusion is that almost every ATM LEC interope with the tested ATM services provided in the ATM network. The problems inflicted in the ATM LAN emulation test depends rather on the ATM LAN emulation configuration than a mismatch in the ATM LANE phase 1 standard. The ATM Forum phase 1 works well according to our tests especially the ATM LAN emulation clients.

The new generation of highspeed networks is most likely develop with support from the IETF (Internet Engineering Task Force). I strongly believe in an market for example TCP/IP over SDH. The support for other network protocols is under progress. The ATM forum unfortunately has the same problems as OSI had in the late 1980's.

4 It-Country

Idé/Concept
Peter Löthberg, Stupi

Testledare/Testmanagers
Monica Bouchebane <monica@netman.ericsson.se>
Per Eriksson, KTH <perixon@dsv.su.se>
Mikael Olsson <micke@ericsson.se>
Assar Westerlund <assar@six.se>

Section 1-7 and **13** written by Patrik Fältström och Lars-Johan Liman
Section 8-12 written by Per Eriksson and Mikael Olsson

Sidor/*Pages*
15

3Com Nordic	Vulkan Kaffe AB
Bay Networks Nordic	F:a Fullgas Motor
Cicso Systems	TreStad Bryggerier AB
Combitech Nexus	CombiSec AB
DES Communications/ UB Networks	NonStop Networks
Digital	AltaVista AB
GE Info Services	Rockville
Media Communications	Smartgate
Microsoft	Vaxholm
NetGain/Verimation/ Signum Support	Förenade Företag
Network Management	Stures Data & Konsult
Salcom	Nordisk Datfisk AB
Sun Microsystems	Sunny Webware AB
TeamWARE	InterTeam AB
Tele2	Svenssons Sop & Sten
Telia	Roffes Räkning & Revision

IT-Country

Contents

Section 1-7 and 13 written by Patrik Fältström and Lars-Johan Liman
Section 8- 12 written by Per Eriksson and Mikael Olsson

1. Introduction

The Interoperabilitet -96 was an event run by the Swedish Network Users Society (SNUS). Each year since 1991, some kind of interoperability tests have been hosted by SNUS. The first two years were targeted to IP-level conformance on the link level, testing things like ISDN and SNA tunneled over IP. Also routing protocols were tested. Later, interoperability tests of Internet mail (RFC-822 and MIME), Firewalls and other link protocols such as ATM have been introduced.

1996 was a year when the tests when a new test was introduced. Part from tests of different products in the classes "Internet Mail with MIME", "Firewalls" and "ATM", a more general test of the knowledge about how to build an Inernet, how to connect a company to Internet, and how to build an Intranet.

2. IT-Country

The main task was to invite the ISPs operating in Sweden, and ask them to first of all extend their backbone to the fair itself. On the floor several "fake" companies (model-companies) were invited, and each one of them had a connection to the Internet via one (or two) of the ISPs. The intention was to test not only the ISPs but also consultants that have knowledge about exactly this problem - how to connect a company to the Internet and publish services on the Internet.

3. Planning

SNUS provided the opportunity for the participants to test their individual products in product tests which were conducted from January to April. Tested products 1996 were firewalls, mail-systems, and ATM/LAN-emulation equipment, see section 2.
IT-Country was built on one week. The infrastructure and network were built on May 6 by the IP-operators and SNUS-NOC. The tests ran the 8th,9th and 10th of May. Some participants arrived late with their equipment and could therefore not participate fully in the test.

4. The model-companies

The model-companies were divided into three classes:

Class 1 - Only a simple connection to the Internet, possible via a modem. They do not publish information, only run protocols like client side HTTP and POP to fetch information from the net. At the fair, these companies had a fixed connection in most cases, because we think the knowledge about how to run PPP or SLIP over a modem is so well known, and the problems one can get because of hardware problems was not something we wanted to introduce.

(Last year we had tests of modem pools, terminal servers, PPP and SLIP, and we saw that the hardware problems with an analogue telephone switch on the fair itself, and make the hardware run was very, very hard, and in real life - most of those problems are already fixed by the local ISP when you get your telephone line.)

Class 2 - A fixed line to the Internet. These companies are probably the most common way of connecting a company to the Internet. The company contact one ISP, gets a domainname, IP address (one "/24" network, formerly called "Class C"), and agrees on if the company itself or the ISP is going to run DNS and other services. Sometimes, the company buys other services from the ISP, such as encrypted lines and gateways between RFC-822 and X.400.

Class 3 - Only three companies were of this class, and of the three, only two participated and reached the goals. The class three companies are connected to two different ISPs at the same time, having services from both (but maybe not at exactly the same time). The idea was to check what kind of redundance you get if you get two connections from two different ISPs compared to having two connections from the same ISP. This is the most interesting setup of the three classes.

The ISPs that were participating was Telia, Global-One and Tele2. They connected each to about 6 "fake" companies. Telia and Tele2 were also responsible for one "fake" company each.

5. Live Backbones

All three ISPs extended their backbone out to the fair, connecting with two full ISDN lines (i.e. a total of 4 times 64kbps per ISP were available). All three of them also extended their AS:es out to the fair, so full routing was available. This last step was not intended from the beginning due to the problems the ISPs would get when they happened to get a full update of the routing tables over the "slow" ISDN link due to some routing flaps. The networks that was available was chosen to really be live, and any mistake could really damage the production in their worldwide backbones. An eloge to the providers for this decision.

The Network Operations Center at the fair (the NOC) was running an exchange point (IX) where the ISPs should connect to exchange traffic and routing information. The NOC also had two ISDN lines to the world (the KTH backbone in Stockholm) but one of them was used as a normal telephone, because the need for a phone was higher than the need for a higher bandwidth than 2*64kbps. The fact that we had one IX (called MIX because the Swedish word for "fair" is "m=E4ssa" so the acronym stands for "M=E4ss-IX") at the fair made the routing more complicated as the ISPs already are connected to at least one more IX, the D-GIX at KTHNOC in Stockholm.

The routing test was because of that to get routing to work as efficient as possible after creating a new global exchange point between ISPs and at the same time adding some customers to the ISPs which are connected to more than one ISP. All of this in one week while tests of higher level services (like RFC-822/MIME mail and HTTP) was done on top of the network.

Locally at the fair, the three ISPs and the NOC had somewhat different hardware. Telia choose to use "digital-x-line" connections to their companies and Tele2 modems, each connecting one central router with one router at the customers site which belongs to the ISP. The customer gets one twisted pair connection at the other side of that router.
Global-One was using one central router and from that one direct twisted pair connections to the "fake" companies. The NOC had one router connecting (with twisted pair) both the NOC backbone and the MIX, to which the other ISPs were connected (see picture number one).

6. Multihomed companies

The network management, and the services that the NOC was running, was done on mainly two Sun workstations. One running NetBSD, the other one Plan97. Network monitoring was done via SNMP on a Macintosh using the software InterMapper and SNMP Watcher. Normal tools like traceroute and ping was of course also used, from both the computers mentioned above, and other x86 based PCs running BSD/OS and NetBSD.

The CAP package was used on the Sun running NetBSD to make it possible to print on an old Apple LaserWriter that only had support for Ethertalk. We were running DNS, HTTP, FTP, Whois++ and SMTP daemons to facilitate the tests at the fair.

Back to the interesting routing setup. Each ISP had their "live" AS extended to the fair, which means that on the MIX, the ISPs were supposed to exchange routing information between the ASes the same way they do at the D-GIX at KTH. The first shot, to make the IP work, was to run EIGRP among all the routers at the fair, but that was a boring exercise. It was different ISPs, so they should run as separate ones.

Day three we started to use BGP4 instead, with live AS numbers. On the MIX, four AS did meet, and the two companies that were connected to two ISPs had their own AS number which forced the ISP and the "class three company" to also echange routing information (more about that later).

7. Best path in BGP4?

According to the theory, BGP4 only selects the best path, and is not doing any load balancing, and that was of course also what happened at the fair. Another theoretical thing we could show was that a company which is connected to two ISPs, one primary and one secondary, should get their IP address out of the CIDR block of the secondary ISP. This because the ISP from which the network is not chosen will make an explicit announcement of the block, and BGP4 will because of that choose that path before the one where the announcement is aggregated into the announcement from the ISP itself. Longest match is what rules, and we could here show that it actually works that way, which not many people have seen live.

The filters that had to be set up between the ISPs was not only simple. This because the ISPs were connected not only at one IX, but two (at least) and as well at the multihomed companies. Assymetric traffic was the result before the routing filters were set up correct - also an interesting exercise for people not working with this daily.

One of the multihomed companies did complicate the situation a little bit more. They had one router connected to each of the two ISPs they were connected to (Telia and Tele2), and each one of those were having its own firewall behind it. Between the two firewalls was an internal network which was setup according to all standard rules regarding DNS, proxies etc. The interesting task here was to exchange routing information between the two routers through the two firewalls. They managed, but due to some bugs in the routing software at one of the ISPs, on the SNMP management software on the NOC, the company was never completely connected to two ISPs. One more day (or maybe one more hour) and even that problem would have been solved.

8. IT- Country testresults

8.1 Objectives And Goals

A real Internet environment is supposed to be simulated. A company is supposed to run basic Internet protocols as access protocols. Which technology the company decides to implement inside its local network is less important.
These tests are built within a working infrastructure of a miniatyr Sweden connected to the internet with full connectivity to the whole internet.

The main goals are to see the skills of the attendees and vendors. and also to see if it is possible to build this environment in such a short time. Also to see that the applications used for the above purpose is compliant.

8.2 Test Managers

Monica Bouchebane	monica@netman.ericsson.se
Per Eriksson	perixon@dsv.su.se
Mikael Olsson	micke@ericsson.se
Assar Westerlund	assar@six.se

8.3 Participants

3Com Nordic
Bay Networks Nordic
Cicso Systems
Combitech Nexus AB
DES Communications/ UB Networks
Digital
GE Info Services
Media Communications
Microsoft
NetGain/ Verimation/Signum Support
Network Management
Salcom
Sun Microsystems
TeamWARE
Tele2
Telia

Vulkan Kaffe AB
F:a Fullgas Motor
TreStad Bryggerier AB
CombiSec AB
NonStop Networks
AltaVista AB
Rockville
Smartgate
Vaxholm
Förenade Företag
Stures Data & Konsult
Nordisk Datfisk AB
Sunny Webware AB
InterTeam AB
Svenssons Sop&Sten
Roffes Räkning & Revision

9. Test Specification

9.1 Basic protocols are as follows:

1 Send and receive mail (preferable RFC-822/MIME)

2 Fetch file from FTP servers

3 Fetch WWW documents from HTTP servers

4 Establish a telnet connection to external telnet servers

5 Fetch articles from NNTP servers

All of these requirements are resolved by set-ups and configurations of a number of systems and protocols, (e.g. SMTP, DNS, FTP, HTTP, NNTP, routing and configuration of firewalls).

9.2 Mail
Send mail from a model-company to all other model-companies i.e all test participants within the Internet provider and across to the other Internet providers. When sending testmail, send a cc: to the test staff. When receiving mail, send a forward to the test staff.

The IT-Country test will test that the mail can be sent and received. The MIME test group will examine the mail during the testdays to see if they fulfill the MIME compliant standard.

9.3 FTP
Fetch file from a ftp server located at another model-company. Send a copy of the fetched file to the test staff. Due to security reasons we discussed with the attendees and decided not to use incoming areas in the FTP-server of the model-company.

9.4 WWW
The purpose of the WWW test is to fetch a http page from the other model-company's web-servers. Those pages shall be sent to the noc via mail to a predefined user. This also requires that the model-companies have a webserver and publish something on it.

The instructions on how to complete these tests and what to do was published on a Interoperability -96 web page at the NOC-server.

The name convention for the model-company web server and the name of the predefined user was given at the NOC-servers webpage.

9.5 TELNET

Login to all other model-companies telnet-servers and create a file with your model-company´s name. The model-company that owns the telnet-server sends the created files to the NOC via mail, with the file as an attachment.
This was our intention but since most of the attending companies are competitors, they didn´t want the others to login to their environment. Some model-companies allowed login but only with encryption keys. Since not everyone had telnet clients that handled encryption keys, we mutually decided not to include telnet in the It-Country tests-96. Hopefully we can include telnet in next years tests.

9.6 NNTP

Due to lack of time we decided together with the model-company not to include news in the IT-Countrytests.

10. Test results

10.1 Test section Mail

This was the first year of testing functions on an infrastructure. We found that has to be very specific in the test procedure and we learned by this the level of specification needed in this type of tests for next year. Most of the tests were specified and most of the companies succeeded in meeting the results.

10.1.2 Test section Mail, configuration

Each model-company shall have a mailalias or a mail recipient:
test@model-companyname.iop.snus.se

All of the model-companies shall send mail to all the others.
Mail should be in MIME-compliant format and include Swedish national characters.

Requirements:
When you send an item of email, ensure that a copy is sent with CC: (carbon-copy) to: *cc@noc.iop.snus.se*

Received email shall be forwarded to: *forward@iop.snus.se*

10.1.3 Test section Mail, results

Since the test contains two parts we hereby publish two test result diagrams.
The first one (table 1) presents the CC: results which show if the model-company have sent test mail or not.
The second one (table 2) presents the FORWARD: which show if test mail has arrived to the specified destination. We know that it has arrived since the mail has been forwarded to us.

10.1.4 Test section Mail, comments

During the tests we had to modify the instructions describing test procedures. As a result of this some of the test data didn't contain the expected information. Therefore this test result may not correspond to what the model-company's really achieved.

10.2 Test section FTP

10.2.1 Test section FTP, configuration

Each model-company shall have a ftpserver with a public area.
On that public area there shall be placed some files that anonymous users can retrieve.
On the NOC's ftpserver there is an incoming area where each company have it's own home directory with two sub-directories "From" and "To". The model-company shall fetch files from all the other model-companies ftpservers and place copies of those files on the NOC's ftpserver in the companies "From" incoming area.

10.2.2 Test section FTP, results

Unfortunately the ftp-specification was a bit unclear.
There has obviously been some misunderstandings about what the NOC meant by companies incoming area at the NOC ftpserver. Some seem to have dropped files in its own companies areas "From" and "To" directories, when others dropped files in the "source-companies" "From" and "To" directories on the noc server.

This is understandable when reading the above. We have to be blamed for this, since the circumstances is as they are, Therefore we have difficulties to present a report on what the different participants achieved.
Next time we have to be more specific where to send the file.

10.2.3 Test section FTP, comments

The test specification was not specific on where the model-companies should put their RTP-files. Several copies were placed as files at the NOC, their own and other companies incoming area.

One thing we could see was that many of the participants seemed to have managed to fetch and drop files from each others ftpservers, and placed copies on the noc server.
Since there were not one place for all files we can't be sure who really succeeded and who failed. Therefore we can not present any table to this test.

10.3 Test section WWW

10.3.1 Test section WWW, configuration

All model-companies shall have a web server with some simple information. They shall also have a web browser able to read web pages, and forward these pages by mail.

Each model-company shall read all the other model-companies test webservers and fetch something from each of those servers. To prove that they succeeded, they shall forward the fetched page by mail to the NOC/test management: *wwwto@noc.iop.snus.se*

10.3.2 Test section WWW, results

Those who participated succeeded in this test, In result table 3 a few x-marks are missing. The model-companies concerned of this fact did not fail to complete the test in any way but due to difficulties mentioned in section 4.6 they did not obtain contact.

10.3.3 Comments

The www-part of the test seems to have been the most simple of them all. We made it a little too simple and next year we have to test more complicated web functions with multimedia and security etc etc.

11 Summary and Comments

Some of the problems the companies ran into were:

- To set up multihoming was more difficult then anticipated. Therefore the participants ran out of time and didn't have time to finish the IT-Countrytest

- DNS configurations

- The internet providers had connectivity problems

- Firewall filtering. Didn't allow different traffic to go through (Mail, Ftp, WWW)

- The model-companies didn't have enough people in the stand or didn't allocate personnel for the IT-Countrytest.

- Since the IT-Country tests were designed and written during the first day of the Interoperability -96 the testspecifications weren't clear about some of the topics. If we had been prepared we would announced the requirements in advance.
(If we had asked the model-companies about telnet we would have known about the security key problems)

Overall every model-company did an excellent job. Since these tests were more or less improvised from the beginning and each of the it-companies test units wasn't informed about how the tests where to be performed, and what we wanted to achieve with these tests.

During this test the participants have proved that they are very good at setting up these types of services, and they are also well aware of the different problems that usually occurs. Therefore we think that the real life customer can require fast installations and services from companies that handles these services in the future.

The suppliers have proved that they would be able too stand up to those demands and requirements, in this topic from good customers specifications.

The test crew want to take the opportunity to thank all of the participants for all the effort that you have spent during the IT-Countrytests.
We are looking forward to meet you next year, and by then we will give you harder tests then this year.

Best regards/
Per Eriksson, Mikael Olsson and Assar Westerlund, Monica Bouchebane

TABLE 1 MAILTESTS CC

CC	TO	Alta Vista	Combisec	Datafisk	Förenade Företag	Fullgas Motor	Interteam	NonStop Data	Roffes Räk & Rev	Smartgate	Stures Data& Konsult	Sunny Webware	Trestad Bryggeri	Vaxholm	Vulkan Kaffe
FROM															
Alta Vista		0	X	X	X	X	X	X	X	X	X	X	X	X	X
Combisec		X	0	X	X	X	X	X	X	X	X	X	X	X	X
Datafisk		X	X	0	X	X	X	X	X	X	X	X	X	X	X
Förenade Företag		X	X	X	0	X	X	X	X	X	X	X	X	X	X
Fullgas Motor						0									
Inter-TEAM		X	X	X	X	X	0	X	X	X	X	X	X	X	X
NonStop Networks		X	X	X	X	X	X	0	X	X	X	X	X	X	X
Roffes Räk&Rev		X	X	X	X	X	X	X	0	X	X	X	X	X	X
Smart-Gate		X	X	X	X	X	X	X	X	0	X	X	X	X	X
Stures Data&Ko		X	X	X	X	X	X	X	X	X	0	X	X	X	X
Sunny Web ware		X	X	X	X	X	X	X	X	X	X	0	X	X	X
Trestad Bryggeri		X	X	X	X	X	X	X	X	X	X	X	0	X	X
Vaxholm		X	X	X	X	X	X	X	X	X	X	X	X	0	X
Vulkan Kaffe		X	X	X	X	X	X	X	X	X	X	X	X	X	0

TABLE 2 MAIL FORWARD

	TO	Alta Vista	Combisec	Datafisk	Förenade Företag	Fullgas Motor	Interteam	NonStop Networks	Roffes Räkn & Rev	Smartgate	Sunny Webware	TreStad Bryggeri	Vaxholm	Vulkan Kaffe
FROM														
Alta Vista		0	X		X					X	X	X	X	X
Combisec		X	0		X		X	X		X	X	X	X	X
Datafisk		X	X	0	X		X	X		X	X	X	X	X
Förenade Företag			X		0			X		X		X	X	X
Fullgas Motor						0								
Interteam		X	X	X	X		0	X		X	X	X	X	X
NonStop Networks			X		X			0			X			
Roffes Räk&Rev									0					
Smartgate		X	X	X	X		X	X		0	X	X	X	X
Sunny Webware		X	X		X		X	X		X	0	X	X	X
TreStad Bryggeri			X		X					X	X	0		X
Vaxholm		X	X	X	X		X	X		X	X	X	0	X
Vulkan Kaffe		X	X	X	X		X	X		X	X	X	X	0

TABLE 3 WWW - TEST

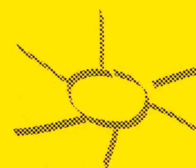
	Websida är hämtad ifrån	Roffes Räkn &Rev	NonStop Networks	Alta Vista	Trestad Bryggeri	Vulkan Kaffe	Svens-sons Sop & Sten	Fullgas Motor	Combi-Sec	Smartgate	Vaxholm	Förenade Företag	Datafisk	Sunny Webware
Företag som har mailat in websidan														
Roffes Räk&Rev		0	X	X	X	X	0	X	X	X	X	X	X	X
NonStop Networks		X	0	X	0	0	0	X	0	X	0	0	X	X
Alta Vista		X	X	0	X	X	X	X	X	X	X	X	X	X
Trestad Bryggeri		X	X	X	0	X	X	X	X	X	X	X	X	X
Vulkan Kaffe		X	X	X	X	0	X	X	X	X	X	X	X	X
Svensson sop&sten		X	X	X	X		0	X		X	X	X	X	X
Combisec		X	0	X	X	X	X	X	0	0	X	X	X	X
Smartgate		X	X	X	X	X	X	X	X	0	X	X	X	X
Vaxholm		X	X	X	X	X	X	X	X	X	0	X	0	X
Förenade Företag		X	X	X	X	X	X	X	X	X	X	0	X	X
Sunny Web ware		X	X	X	X	X	0	X	X	X	X	X	X	0

13. Conclusions

What are the conclusions then. First of all, one do not get what one want with multihoming to more than one ISP. Of course, one solve some other kind of redundance than when one connect with two lines to the same ISP, but because of the lack of load balancing in BGP4, the backup link is only a backup link - which probably costs to much to have. Having two lines to the same ISP makes it possible to participate in the same AS as the ISP, and because of that use the two lines more efficient. If a customer have their own AS number (as probably the case when doing this kind of multihoming) he has to be prepared of really participating in the manual setup of the routing filters between the AS clouds as is happening today. He basically becomes a small ISP himself.

The ISPs participating at the fair also pointed out that this multihoming is nothing they have in their pricelist, and nothing they recommend any customer. Maybe very large organizations, such as a multinational company, or the national defense or such, can be connected to more than one ISP, but the question is still if this have to mean that every computer on the customers network can reach the outer world through any of the two links? That is probably not what they really want because the setup is very, very complicated. It is much easier - especially internally for the customer - to have one default route for each point on their network.

5 internetdagen



3Com Nordic
AU- SYSTEM
Bay Networks Nordic
Cisco Systems
Combitech Nexus
DES Communications
Digital Equipment
GE Info Services
Global One/France Telecom
Media Communications
Microsoft
Netgain
Network Management
Salcom
Signum Support
Sun Microsystems
TeamWARE
Telia
Tele2
UB Networks
m fl

Internetdagen

1 Inledning

Internetdagen genomfördes för första gången under Interoperabilitet-96. Företag och personal som arbetat med IT-Country presenterade under en sista, tredje dag, uppbyggnad, testförfarande och resultat som framkommit under Interoperabilitet-96.

2 Syfte

Idén om en tredje dag - Internetdagen - har med tiden vuxit fram i diskussion med de leverantörer/utställare som deltar under Interoperbilitetsdagarna. Huvudsyftet med Internetdagen var att presentera resultatet av Interoperabilitetstesterna för en bredare allmänhet än den som besöker Interoperabilitet.

3 Målgrupp

- Människor som arbetar med datakommunikation men inte har tid att komma under två dagar

- Kunder till utställarna som vill se vad deras leverantörer egentligen kan

- Högre chefer, opinionsbildare och beslutsfattare

- De som är intresserade av området men som inte arbetar på den specialiserade teknikernivå som dem som vanligtvis besöker Interoperabilitet.

4 Genomförande

Genom att i en pedagogisk form dela ut resultaten till besökarna samt att ordna guidade turer i IT-Country förmedlades vad som fungerade resp inte fungerade i IT-Country.
Vidare presenterades resultatet för beslutsfattare från företag och organisationer. Detta bla för att visa effektiva sätt att bygga upp internet-tjänster på sina respektive hemmaorganisationer.
Internetdagens program varvades med korta föredrag av gästtalare, presentationer av testresultat och guidade turer. En VIP-lunch för speciellt inbjudna ordnades.

5 Marknadsföring

Utställarföretagen fick 200 biljetter eller fler att dela ut till kunder och andra intressenter. Annonsering skedde i Datateknik med ett special-erbjudande till dess prenumeranter. Tre annonser vardera i Ny Teknik samt i Dagens Industri publicerades i slutet av april/ början av maj. Vidare spreds informationsfoldrar och affisher via utställarföretagen.

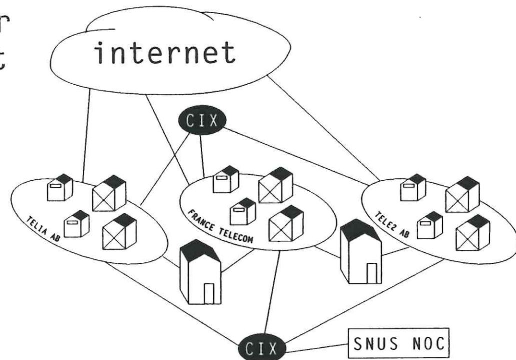
Morgondagens nätverk, idag!

I maj 1996, bygger Sveriges data-, och nätleverantörer upp en framtida infrastruktur med nät och tjänster.

Fredagen den 10 maj har du möjlighet att besöka IT-COUNTRY

- en modell av Sveriges framtida infrastruktur.

Ta del av resultatet och deltagarnas erfarenheter efter genomfört arbete.



Möt de tekniker och utställare som kommer att bygga morgondagens nätverk.

Diskutera Internet på en professionell nivå och lär för framtiden.

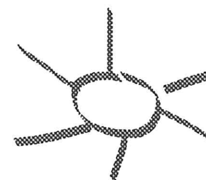
GUIDADE VISNINGAR

Se och förstå IT-COUNTRY med hjälp av guidade turer. Swedish Network Users Society, Snus, anordnar visningar varje heltimme.

Resultatet av arbetet i IT-COUNTRY presenteras och du får en teknisk dokumentation.

Ett varierat aktuellt program under hela dagen.

Happenings!



internetdagen

Internetdagen vänder sig till

- dig som arbetar med datakommunikation men inte har tid att gå på seminarier och kurser.
- dig som arbetar på chefs/managementnivå i ett företag med intern nätkommunikation
- dig som ligger i förhandling om nätverk
- dig som är kund – eller planerar att bli kund – till någon av utställarna
- opinionsbildare/politiker med intresse av IT-utveckling

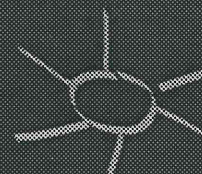
Besök internetdagen och du får en effektiv inblick i morgondagens IT-möjligheter och en kunskap som ligger steget före.

Sollentunamässan
10 maj 09.00 – 15.00

Begränsat antal platser.
Reservera plats nu.

SWEDISH NETWORK USERS SOCIETY & DATATEKNIK

inbjuder till en visning av framtidens nätstruktur på



internetdagen

ett evenemang i samband med INTEROPERABILITET-96
Sollentunamässan 10 maj kl 09.00-15.00

- Se **IT-COUNTRY** - framtidens infrastruktur.
- **PRESENTATION** av arbetet i IT-Country
- Möt de leverantörer och tekniker som kommer att bygga **SVERIGES FRAMTIDA NÄTVERK.**
- Diskutera **INTERNET PÅ EN PROFESSIONELL NIVÅ** och lär för framtiden.
- Ett varierat **AKTUELLT PROGRAM** under hela dagen.
- Happenings!

Guidade visningar, varje heltimme, av representanter från **SWEDISH NETWORK USERS SOCIETY (SNUS),** samt teknisk dokumentation.

Erbjudande!!!

Exklusivt för dig som prenumererar på DATATEKNIK.
Du får två biljetter till priset av en (ord. pris 200:-).
Ta med dig en kollega och lär för framtiden. Begränsat antal platser!

☐ Ja, jag är intresserad och vill ha ett program.
☐ Ja, jag önskar två biljetter till priset för en. Totalt 200 kronor.



internetdagen

Namn ______________________________

Företag ______________________________

Adress ______________________________

Tel/Fax ______________________________

E-post ______________________________

Skicka/faxa till: Internetdagen co/Snus • Box 396 • 101 27 Stockholm
Tel 08-665 60 53 • Fax 08-665 80 48 • E-post <I96@snus.se>

PROGRAM

Internetdagen

09.00	Internetdagen öppnar
09.30	Musiknet, ett projekt att kommunicera med musik över Internet. Ett samarbetsprojekt mellan Skolverket, SR, Musikhögskolan mfl Talare: *Greg Fitzpatrick*
10.00	Guidad visning 1 Ansvarig: *Patrik Fältström*
10.30	Internet - Företagsledningens perspektiv. Talare: *Roland Acra*, Cisco, Frankrike
11.00	Guidad visning 2 Ansvarig: *Östen Frånberg*
11.30	Prel testresultat IT-Country: *Östen Frånberg & Patrik Fältström*
12.00	Guidad visning 3 Ansvarig: *Lars Beijar*
13.00	Guidad visning 4 Ansvarig: *Lars-Johan Liman*
13.30	Prel testresultat IT-Country: *Östen Frånberg & Patrik Fältström*
14.00	Guidad visning 5 Ansvarig: *Kjell Gustafsson*
14.30	*Östen Frånberg* avslutning

Biljetter kan beställas från
Internetdagen co/Snus
Box 396 • 101 27 Stockholm

6 ÖVRIGT

TIDNINGSARTIKLAR

"Snus bygger Sverige i miniatyr på Internet"
Nätverk & Kommunikation, nr 6 juni -96

"Svensk internetutbyggnad i återvändsgränd"
Datateknik, nr 1, jan -96

"Svårt med Internet i två moln"
Dagens Data, specialtidning på Interoperabilitet-96, Datateknik maj-96

"Mässnätet på Interop-96"
Datateknik, nr 10, maj-96

"Enklare e-post med gemensam standard"
Ny Teknik, jan-96

"Enlighet om dator - postadresser"
Datateknik, nr 1, jan-96

"Samtrafik mellan mailsystem"
Kontakten, vinter, -96

"SNUS bygger realistiskt nätlandskap direkt på mässgolvet"
Nätvärlden, nr 3, april -96

"Framtidens routing fungerar"
Datateknik, nr 10, juli-96

SEMINARIEPROGRAM

Teknik och management, 8-9 maj-96

KEYNOTESPEAKERS

Peter Löthberg, Stupi AB
Johan Särnquist, AB Electrolux
David Partain, SNMP Research Europe
Anders Hillbo, KTH, NADA
Ann-Marie Nilsson, STATTEL-delegationen

SÄRTRYCK UR NÄTVERK & KOMMUNIKATION 6/96
Publikation utgiven av IDG världens största utgivare av datarelaterad fackpress

INTEROPABILITET – EN LYCKAD MÄSSA. Interopabilitet är en mässa med nätverkstester och seminarier. SNUS, Swedish Network User Society, anordnar den sedan fem år tillbaka. Förberedelserna har varit noga och de tre nätverken, som företagen kan ansluta sina system till, började byggas upp redan den andra maj i år. Bytet av lokal till Sollentunamässan var ett lyckat grepp. SNUS ordförande **Östen Frånberg** är nöjd med årets mässa.

SNUS byggde Sverige

i miniatyr på Interop

Bättre organisation och bättre lokaler utmärkte årets Interoperabilitet. Det gav att modellföretagen som byggdes upp hade lättare att kommunicera med varandra och ut på Internet.

En av huvudattraktionerna på årets Interop var testnätet i sig. Nätverket var nämligen uppbyggt som ett Sverige i miniatyr och kallades IT Country. Det fanns tre operatörer som byggde upp varsitt litet nät och till de näten kunde de andra utställarna på mässan ansluta sina system.

Utställarna på mässan byggde upp egna modellföretag som skulle simulera trafiken från ett visst sorts företag. Här fanns de små familjeföretagen upp till företag som om de existerade skulle ha flera hundra anställda.

Varje modellföretag anslöts till en operatör utom några som kördes mot flera. Operatörerna skapade sedan en koppling mellan sig själva och även ut på det vanliga Internet.

Modellföretagen kunde sedan kommunicera mellan varandra och med andra via operatörernas nät. De tester som gjordes var bland annat att skicka e-post till varandra, hämta information från Webservrar och lägga upp filer på FTP-servrar. Exakt hur testerna utföll var inte klart när detta skrevs. Några större problem lyckades inte Nätverk & Kommunikation höra om när vi pratade med en del av deltagarna.

Färre problem

En av de stora överraskningarna på mässan var kanske att det här verkar ha fungerat utan större problem. Annars brukar Interoperabilitet vara förknippat med utställare som förtvivlat försöker få sina system att fungera.

En förklaring till att det mesta verkar ha fungerat bättre i år är att förberedelserna har varit bättre. Man har helt enkelt lärt av misstagen.

– Vi började bygga nätet redan den andra maj i år, säger **Östen Frånberg**, ordförande i SNUS. Då kom operatörerna hit och satte upp sina nät och stamnätet var klart när de andra leverantörerna kom med sin utrustning.

Även bland utställarna verkade de flesta vara nöjda med hur nätet fungerade.

Lite krångel och bättre lokaler

– Det har faktiskt aldrig varit så litet krångel under de år vi varit med, säger **Johan Pihlsgård** på Salcom. Vi fick i och för sig låna ut alla maskiner vi skulle ha med och låna in nya, men det gick att få upp allt på en halv dag ändå.

En nyhet på årets Interoperabilitet var lokalen. I år var det Sollentunamässan som gällde och det gav betydligt mer utrymme än tidigare.

Årets val av lokal för mässan gjorde att alla utställare och testare fick gott om plats och slapp gömma sig i diverse skrymslen som tidigare. Alla tester utfördes inför öppen ridå och besökarna kunde se hur testerna utfördes.

– Det är ett mer öppet och mer roligt forum i år än tidigare och folk kan komma fram till oss på ett helt annat sätt när vi sitter och jobbar med testerna, säger **Helen Svensson** på Tele2.

Stommen i Interoperabilitet har varit seminarier och tester under åren och så var det i år också. I år testades, förutom testerna inom IT Country, e-postsystem, brandväggar och ATM/LAN-emulering. Borta var alltså det traditionella routertestet.

I testerna för e-post och ATM/LAN-emulering klarade de flesta leverantörer sig riktigt bra. De testkriterier som satts upp klarades till allra största delen av flertalet.

På ATM-sidan till exempel kunde i stort sett alla ATM-produkter kommunicera med varandra. De problem som fanns låg inte i själva ATM Lane e phase 1-standarden utan snarare i konfigurationen av produkterna.

Slutsatsen blev att ATM Forum Phase 1 fungerar bra idag och kan användas fullt ut. Fortfarande är det inte hundraprocentigt säkert att alla produkter kan kommunicera med varandra så en viss försiktighet vid inköpen krävs än.

Brandväggarna kraschade

Brandväggstestet gick naturligt nog ut på att försöka slå hål på brandväggen. Metoden här har var främst att ge sig på den dator brandväggen kördes på snarare än brandväggen i sig.

Testarna letade efter hål i operativsystemen på de datorer som brandväggarna kördes på och försökte komma in den vägen.

Det var samma sätt som en cracker förmodligen skulle använda. Varför brottas med en kraftfull brandvägg när du kan ge dig på det betydligt sämre skyddade operativsystemet Resultatet blev väl inte helt lysande för deltagarna.

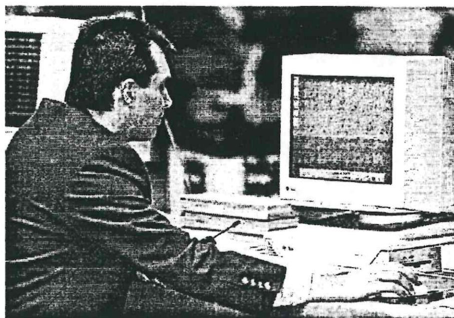
fortsättning på sid 65 ▶

SNUS

SNUS står för Swedish Network User Society. Organisationen bildades 1991 och hade som en av de ursprungliga målsättningarna att få någon att starta ett kommersiellt IP-nät i Sverige. Något de också lyckades med i och med att Tele2 drog igång Swipnet. Idag har SNUS över 110 företag som medlemmar. Bland medlemsföretagen finns allt från de största svenska företagen till fåmansföretag. Ledningen sitter personer som till vardags arbetar med datakommunikation på företag som Ericsson, Telia och Sics. Det som SNUS är mest känt för är att de arrangerar Interoperabilitet. En mässa med tester och seminarier som ägt rum varje år sedan 1991.

STORT INTRESSE. **Rolf Schu[illegible]** [illegible] och **Jöns [illegible]chan** från GE Info är alla [illegible] deltagare [illegible]an. Här är de med **Lar[illegible]** från ASG.







NÄTANSLUTNA I VIMLET. **Patrik Fältström, Hans Strömgren, Pavol Simai** och **Ludmila Ottova** var alla intresserade av att ge sig i kast med nätverken på mässan.

– Vi kunde inte komma innanför någon av brandväggarna, men vi lyckades sätta ner tillgängligheten på i stort sett alla, säger testledaren **Staffan Hagnell** på Network Management.

Det gick att irritera brandväggarna så de blev för belastade för att släppa in de som hade behörighet. Inte lika allvarligt som om någon skulle ha kommit in, men det gör ju nätet oanvändbart för behöriga användare. Att testarna inte lyckades ta sig innanför brandväggarna är i sig heller ingen garanti för att de är helt säkra.

– Vi hade inga klienter som körde innanför brandväggarna och det är ju den naturliga angreppspunkten annars, säger Staffan Hagnell.

Ett resultat av testerna kommer förmodligen att bli att en svensk organisation för nätsäkerhetsfrågor bildas. En sorts svensk motsvarighet till Cert verkar vara på gång.

– Det behövs mer arbete med nätsäkerhet i Sverige så i början i juni ska vi mötas några stycken och diskutera, säger Staffan Hagnell.

Organisationen skulle bland annat fungera som ett nätverk för utbyte av information om nätsäkerhet bland de deltagande företagen. Liknande organisationer finns redan för mer fysisk säkerhet och nu är det förhoppningsvis dags för nätverken att få sin beskärda del också.

Seminarieprogrammet innehöll förstås seminarier som anknöt till de tre testområdena. Därutöver fanns det seminarier om World Wide Web, Internets utveckling och elektroniska pengar. Något officiellt besökarantal för Interoperabilitet 96 fanns inte vid denna tidnings publicering. SNUS ordförande **Östen Frånberg** var dock nöjd med uppslutningen.

– Jag uppskattar att det var ungefär 600 personer här första dagen med utställarna inräknade och det är jag mycket nöjd med, säger han.

Litet smolk i glädjebägaren fanns det dock. Bland annat var det inte alla företag som ville vara med på mässan.

– Det är beklagligt att vissa företag inte vill ställa upp med sina produkter och låta dem testas här, säger Staffan Hagnell.

En del leverantörer verkade sköta sitt deltagande på Interoperabilitet med vänster hand.

– Jag skulle vilja se litet mer engagemang från vissa av deltagarna, säger **Per-Olof Johansson** på Tele2 utan att närmare gå in på vilka som åsyftas. Nu går det för lösa boliner på sina håll vilket ställer till problem för oss andra.

Ett klagomål som Interoperabilitet fått i stort sett alla år är att testrapporterna har dröjt länge. Det hoppas man ha kommit till rätta med i år.

– Preliminära testrapporter finns klara redan nu och presenteras under Interoperabilitet 96, säger Östen Frånberg.

De kompletta testrapporterna ska förhoppningsvis dyka upp snart. Den som vill läsa dem kan titta på SNUS hemsida där de kommer att dyka upp när de är klara. Hemsidan finns på: **http://www.snus.se/SNUS/**

Kent Olofsson

Experternas dom:

SVENSK INTERNET-UTBYGGNAD I ÅTERVÄNDSGRÄND

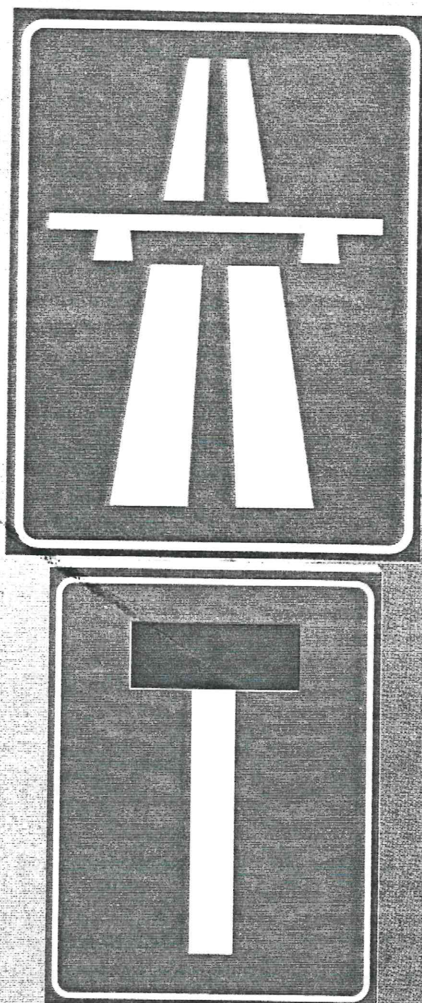


ILLUSTRATION: INGEMAR FRANZÉN

Att vi ska få informationsmotorvägar i framtiden har väl knappast undgått någon svensk. Men att bygget redan pågår är mindre känt. Nästan hälften av Sveriges kommuner är på väg in i stora satsningar som enligt kritiker mycket väl kan leda helt fel.

Enligt en rapport från Nutek som kom ut i slutet av förra året är det till exempel ett hundratal kommuner som endera bygger eller planerar att bygga egna datanät. I första hand byggs näten för att klara de interna kommunikationsbehoven, men så gott som samtliga kommuner är också anslutna till externa datanät som Internet. Om inget oförutsett inträffar kan den svenska delen av Internet alltså komma att härbärgera ytterligare några hundratusen användare inom en nära framtid.

Vid sidan av kommunerna finns Skolverkets skoldatanät, dagstidningar som säljer Internetåtkomst, en flora av samverkande First Class-BBS:er som erbjuder Internetanslutning och mycket annat.

Faktum är att utvecklingen går så snabbt att en några av Sveriges ledande Internetexperter är allvarligt oroade för att den kommer spåra ur. Det är dags att ta ett halvt steg tillbaka och börja fundera på hur man ska lägga grunden för denna expansion, innan vi blir sittande med isolerade öar som bara med stora ansträngningar kan fås att kommunicera med varandra, hävdar de.

Enligt Nutekrapporten är bristen på kompetens det största hindret för en ökad användning av informationsteknik i kommuner och företag. Alla sorters kompetens saknas, både hos användarna och hos den personal som ska köpa in och förvalta utrustningen.

– Mycket av de pengar som kommunerna just nu investerar i egna nät kan visa sig vara kastade i sjön. Det är stor risk att de kommer få börja om från början, säger Peter Löthberg, en av Sveriges ledande Internetexperter.

– Staten borde ha tagit tag i problemet med den logiska infrastrukturen för länge sedan. Det börjar bli bråttom; min bedömning är att vi har ett eller högst två år på oss innan vi börjar få kvalitetsproblem orsakade av felaktig nätbyggnad. Och det kan drabba telefonerna lika väl som datakommunikationen, säger Mats Brunell på Stiftelsen för kunskaps- och kompetensutveckling (KKS).



– Vi har bara sett början av skalningsproblemen. Det bara är 6-7 procent av befolkningen som använder e-post idag, hälften kan komma göra det vid sekelskiftet och dit är det bara fyra år, säger Mats Brunell vid KK-Stiftelsen. FOTO: PER WESTERGÅRD

– Vi har bara sett början av skalningsproblemen än. Tänk till exempel på att det bara är 6-7 procent av befolkningen som använder e-post idag. Det är inte orealistiskt att anta att hälften kommer göra det vid sekelskiftet och dit är det bara fyra år.

Kritikerna pekar på tre problem. Det första är den fysiska infrastrukturen, hur flera rikstäckande driftsäkra nät ska byggas, och framför allt: vem ska betala för det. Till samma område hör frågor om hur man ska säkerställa en någotsånär jämlik åtkomst till nätet.

Det andra problemet är hur information ska organiseras för att bli överblickbar – om ingenting görs kommer Internet bli en gröt av osorterad information, omöjlig att navigera i. Och man bör ställa krav på att åtminstone den offentliga informationen struktureras på ett sådant sätt att medborgarna har lätt att hitta.

Den tredje typen av problem är något svårare att sätta fingret på, men det handlar om att man måste tillämpa etablerade metoder för att bygga stora datanät. Dessa metoder är välbekanta för dem som har varit med och byggt det globala Internet, men konsultföretagen och kommunernas IT-ansvariga har många gånger inte kläm på hur det ska gå till. Det kan till exempel vara en sådan sak som att strukturera sitt IP-nät så att det går lätt att byta Internetoperatör, eller att ansluta sig till två operatörer samtidigt.



– Mycket av de pengar som kommunerna just nu investerar i egna nät kan visa sig vara kastade i sjön. Det är stor risk att de kommer få börja om från början, säger Peter Löthberg, en av Sveriges ledande Internetexperter.

– Den som lyssnar på Telia kan få intrycket att ISDN eller ATM är lösningen på alla problem, men bådadera är egentligen bara en ny sorts sladd. Det som måste till är en kommunikationsarkitektur ovanpå dem, som omfattar alla typer av nät byggda med olika typer av sladd, säger Peter Löthberg.

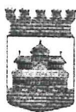
– Om man vill ha en öppen och icke leverantörsberoende arkitektur finns det TCP/IP (Internet) och OSI att välja på, och OSI är det knappt någon som satsar på längre. Alltså är det bara Internet kvar.

I ett PM räknar Mats Brunell upp några problem som måste åtgärdas innan Internet i Sverige har vuxit sig alltför stort för den nuvarande infrastrukturen. Det gäller framför allt att få operatörerna att samsas kring en gemensam, konkurrensneutral hantering av nätnamn och -adresser, vägvalssystem (routing) samt säkerhet och tillhörande kryptonyckelhantering.

För att nätet ska bli driftsäkert och klara de kommande trafikvolymerna måste det byggas flera hopkopplingspunkter där operatörerna kan utväxla trafik. Idag finns det en sådan punkt i Sverige, på KTH i Stockholm, varifrån också alla länkar från Sverige till andra länder utgår. Var de nya hopkopplingspunkterna ska ligga, hur de ska finansieras och hur driften ska organiseras bör operatörerna själva kunna komma överens om.

fortsätter på nästa sida

Tre kommuner – tre olika lösningar



Helsingborg har ett stadsnät som förbinder många av kommunens förvaltningar. Det är Telia som är nätoperatör och även står för det fysiska transmissionsnätet.

– Vårt första och viktigaste beslut var just att inte bygga nätet själva utan istället abonnera på en nättjänst, berättar IT-chefen Troed Troedsson.

– En stad av Helsingborgs storlek har svårt att hålla sig med rätt kompetens för att driva ett nät och hänga med i utvecklingen.

Telia har byggt Helsingborgs stadsnät som ett ATM-nät, men den tjänst som kommunen köper är lokalnätsanslutningar. I abonnemangsavtalet står ingenting om vilken teknik som ska användas.

När nätet togs i drift i februari 1995 började man med att lyfta över 15 anslutningar från ett gammalt nät, och det fungerade över förväntan.

– Hittills har vi ingen anledning att ångra oss. Vi har lika bra nät som tidigare till en mycket lägre kostnad – 20 000 kronor per anslutningspunkt och år och ingen trafikavgift, säger Troed Troedsson.

Stadsnätet är länkat till Internet via kommunens energibolag, som också är lokal Internetoperatör och länkad till Tipnet. □



Stockholms svar på utmaningen hur man bygger nät heter Stokab. Bolaget, som ägs av kommunen, har i uppdrag att bygga ett fibernät som når alla kvarter i innerstaden och arbetsplatsområden i förorterna. I det fibernätet får sedan Internet-, tele- och kabelTV-operatörer hyra plats.

För att kunna göra sitt jobb har Stokab fått tillgång till stadens alla tunnlar och avloppsledningar, samt till tunnelbanan. Totalt handlar det om ungefär fem mil tunnlar och 60 mil rör – en siffra som bara Telia kan komma i närheten av.

Stokab tjänar två syften. Det ena är helt enkelt att undvika att alla dessa operatörer begär att få gräva upp gatorna för att lägga sina egna sladdar, det andra är att etablera en spelplan där operatörerna kan konkurrera på lika villkor.

– Alla operatörer ska kunna få en kabel till kunden, så att ingen kan äga sin abonnent genom att äga sladden, har Stokabs Sverker Lindbo en gång beskrivit affärsidén.

Kommunen själv driver inget nät, utan tänker köpa nättjänster av de operatörer som hyr fiber av Stokab. □



Kiruna hyr Telias kablar till stadens IP-nät Linnéa, som förbinder ett antal skolor och förvaltningar i kommunen. Däremot sköter kommunen nätdriften, via stiftelsen TECEK (Tekniskt Centrum i Kiruna) som man äger tillsammans med LKAB och andra lokala företag.

– Vi började i liten skala för ett år sedan. Allt som allt kostade Linnéa högst en miljon kronor, säger Börje Wiss som är vd för stiftelsen.

– First Class var ett av de alternativ vi tittade på, men vi kom fram till att Internet skulle täcka mer av våra behov.

Den första miljonen kom dels från kommunen, dels från länsstyrelsen. Men Linnéa drar också in pengar på att sälja Internetabonnemang: omkring 200 privatpersoner och fem eller sex företag har nappat under det första året. Enligt Börje Wiss behöver man ytterligare några abonnenter för att det hela ska gå runt.

– Kommunens mål är att Internet ska vara så billigt att vem som helst ska kunna ansluta sig. Det ska inte vara förbehållet de betalstarka grupperna, säger Börje Wiss.

Ett privatabonnemang kostar 200 kronor i anslutningsavgift och därefter 100 kronor per månad. Ingen timtaxa tas ut. □

Forts. Komprimera...

Sist men inte minst påpekar Mats Brunell att lagstiftningen måste ändras, så att det ställs krav på Internetoperatörerna på samma sätt som Telelagen ställer krav på teleoperatörer. För att få kalla sig Internetoperatör och sälja tjänster ska man vara tvungen att bidra till de gemensamma funktionerna och ha ett standardiserat produktutbud.

– Jag tycker inte att Internetmarknaden fungerar i Sverige idag. Köparna vet ofta inte vilka krav de ska ställa. Det måste vara bättre att lära dem vad de ska kräva än att koncentrera sig på att göra det lätt för operatörerna, säger Peter Löthberg.

– Att ta hjälp en konsult kan förstås vara en tillfällig lösning, men se i så fall till att det blir någon som har varit med på IETF-möten och försökt sätta sig in i Internettekniken. Annars är det bättre att lära sig själv än att betala konsultens utbildning.

Den långsiktiga lösningen på problemet med bristande kompetens är naturligtvis utbildning. Ju mer spritt Internet blir, desto fler kommer att lära sig hur det fungerar och vad man ska kräva som köpare av Internettjänster. För att snabbt komma igång med utbildningen håller nätanvändarföreningen Snus på att ta fram en katalog där man beskriver hur tre typiska Internetanslutningar kan se ut: ett liten organisation (högst 10-15 personer), en medelstor samt en stor med enheter på flera orter och med anslutning till mer än en operatör.

Tanken är att den som vill beställa en Internetanslutning ska kunna plocka fram det exempel som passar bäst in på den egna organisationen och gå till operatörerna och säga "det här vill jag ha". Hur typfallen kan fungera i praktiken kommer Snus att demonstrera på Interop, föreningens årliga utställning, som i år ska handla om Internetanslutningar och -tjänster.

– Tricket är att förpacka i princip komplexa tjänster på ett sådant sätt att folk inte behöver förstå tekniken inuti burkarna, säger Peter Löthberg.

– Jag skulle vilja se ett väldefinierat gränssnitt mellan kund och operatör som man kan peka på och säga "det här är en IP-tjänst". Ungefär som alla vet att ratten ska sitta framtill och gaspedalen längst till höger i en bil.

Trafikkapaciteten i stamnäten inom Sverige är inget omedelbart problem. Telia, Banverket med flera har lagt ut rejält med fiberkabel och utnyttjar inte mer än några procent av sin kapacitet. Transmissionsnätet, dvs den del av telenätet som kopplar ihop telefonväxlarna, är digitalt i så gott som hela landet.

Problemet är snarare att kunna erbjuda bandbredd till rimlig kostnad även för andra användare än företag inne i stora tätorter. I storstäderna är det full konkurrens mellan operatörerna men på mindre orter, i synnerhet i norra Sverige, har Telia i praktiken monopol och sätter priserna därefter.

Att bygga ut informationsmotorvägarna så att de täcker hela Sverige kostar förvisso pengar, men mindre än vad väg- och järnvägsbyggen tillåts kosta. Under de närmaste åren plöjs omkring 25 miljarder ner i motorvägar och järnvägar för att förkorta restiderna runt Mälaren och till Arlanda.

Regeringen har nyligen utrett behovet av en fjärde marksänd TV-kanal, och i det sammanhanget passade åtskilliga remissinstanser på att påpeka det okloka i att investera ännu mer i ett analogt nät när den digitala tekniken inte bara står för dörren utan har klivit in i farstun. Det går att spara pengar genom att samordna TV-nätet med andra instanser som behöver egna rikstäckande nät.

– Att i dagsläget fatta beslut om en ny marksänd analog kanal vore olyckligt. En av de stora infrastrukturfrågorna är nämligen om TV ska gå i egna kablar eller inte, säger Mats Brunell.

En motsvarande utredning i Finland slutade, enligt en artikel i Svenska Dagbladet, med att utredaren förespråkade ett markbundet digitalt distributionsnät.

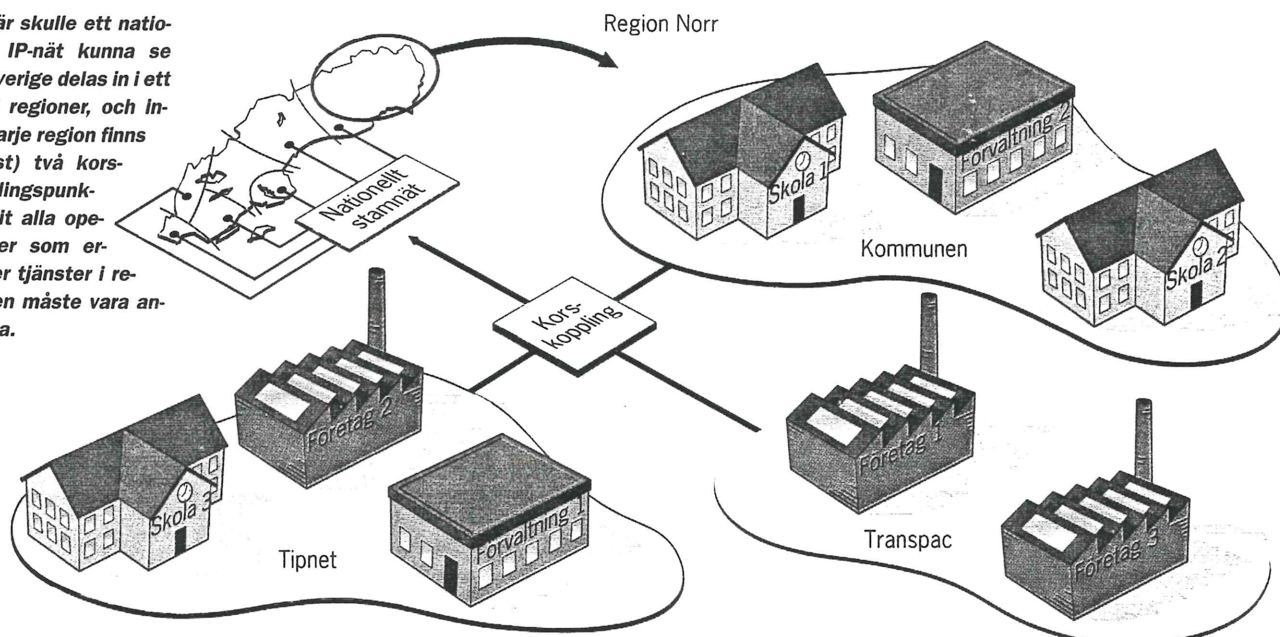
– En tanke kan vara att samutnyttja försvarets telenät på de platser där det finns, för att den vägen ge glesbygden tillgång till telefoni, säger Peter Löthberg.

Sveriges Television och TV4 betalar kring 200 miljoner per år och kanal för att sända ut sina TV-program. Dessutom har SvT ett internt nät för att sända program mellan distrikten. Tillsammans kostar detta strax under en miljard kronor per år i drift – att jämföra med till exempel de 25 miljarder som investeras i Mälardalens fysiska kommunikation. I princip är det inget som hindrar att TVs nät också används för datakommunikation och telefoni, men för att en sådan struktur ska kunna komma till stånd måste någon, lämpligen staten, ta ett samordningsansvar.

LENNART PETTERSSON

Ett nationellt nät

Så här skulle ett nationellt IP-nät kunna se ut. Sverige delas in i ett antal regioner, och inom varje region finns (minst) två korskopplingspunkter dit alla operatörer som erbjuder tjänster i regionen måste vara anslutna.



Trafik mellan regionerna överförs i särskilda "långdistansnät" vars enda uppgift är att förbinda korskopplingspunkterna med varandra – det är för övrigt den modell som används inom USA.

Vid sidan av den gemensamma nationella strukturen kan operatörerna naturligtvis bygga egna rikstäckande nät.

Bilaterala avtal, där två operatörer kommer överens om att installera en direkt länk mellan varandras nät är också tillåtna – så länge alla dessutom är anslutna till de föreskrivna korskopplingspunkterna.

Driftsäkerheten blir bättre än i det nuvarande nätet där det finns en enda korskopplingspunkt för hela Sverige, men även bortsett från detta finns det fördelar med att bygga nätet på det här sättet. En är att det ger regionala operatörer en chans att konkurrera, i och med att de får access till övriga Sverige och hela Internet på samma villkor som de stora aktörerna.

En annan och kanske viktigare poäng är att IP-adresser med den här modellen kan delas ut regionalt istället för per operatör. En användare som byter operatör behöver alltså inte dessutom byta IP-adress – försåvitt han eller hon inte samtidigt flyttar till en annan del av landet.

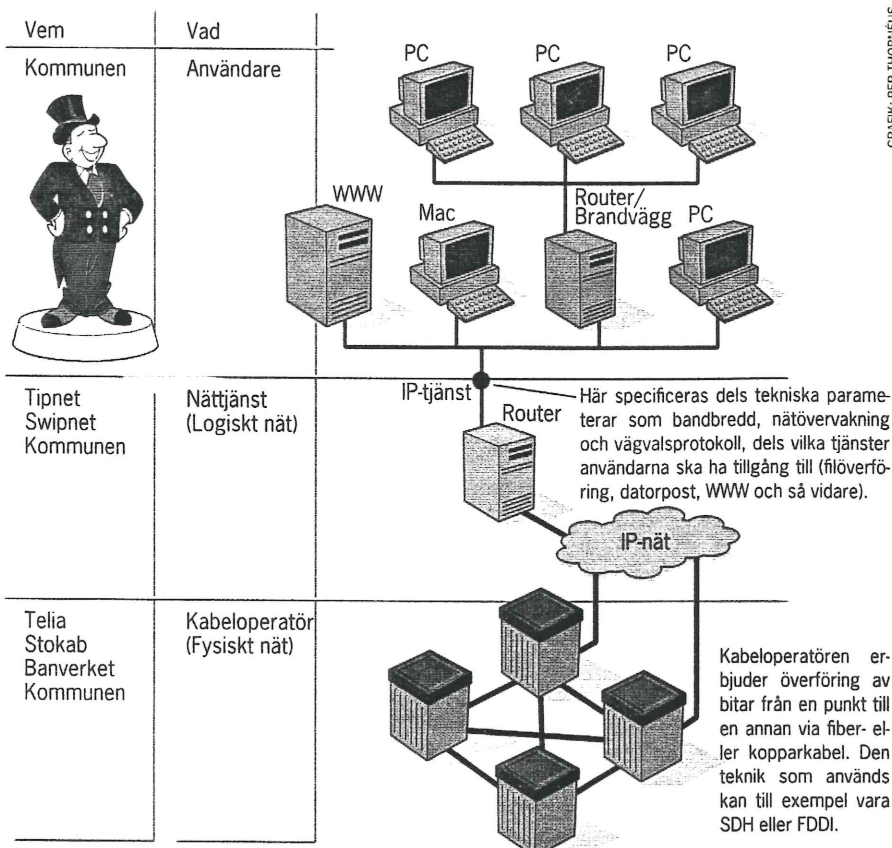
För att det ska fungera smidigt måste operatörerna också samarbeta kring vissa centrala nätfunktioner som katalogtjänster och vägvalsfunktioner. □

Den kloka IT-kommunen

Alla artiklar och diskussioner om datakommunikation lutar sig på ett eller annat sätt på den så kallade OSI-modellen med dess sju "lager" av kommunikation. För praktiskt bruk är den dock onödigt finkornig; det räcker med den förenklade treskiktsmodell som används i figuren här intill: som användare köper man Internettjänster av en nätoperatör som i sin tur hyr transmissionskapacitet från en kabeloperatör.

Experternas främsta råd kan uttryckas väldigt kort: håll isär de tre skikten och se till att det är rena gränsytor mellan dem! Då kan uppgifterna utföras av olika organisationer och då kan man som användare byta nätoperatör utan att behöva göra om allt för mycket i det interna nätet.

Problemet för många kommuner är att man har användare som ska anslutas men saknar kabelkapacitet. Offerter från hugade kabeloperatörer visar kanske att det blir billigast att dra kabel i egen regi. Efter att ha kopplat ihop de egna förvaltningarna i ett nät sätter man in en modempool och börjar sälja Internetaccess till privatpersoner och lokala företag – personalen och större delen av den utrustning som behövs finns ju ändå på plats. Och helt plötsligt är kommunens dataavdelning en Internetoperatör med allt vad det innebär.



GRAFIK: PER THORNÉUS

Dagens Data

Producerad för
Interop -96
av
Datateknik

Se upp med överskattad brandvägg

Idag lämnade Microsoft slutligen in sina MIME-tester på sin Exchange Server. Årets produkttester skulle vara inlämnade i förväg – senast 25 april om man ville ha sina resultat evaluerade.

Snus kan endast lämna partiella rapporter om läget för årets produkttester. MIME-testerna är inte utvärderade och ingen vill uttala sig om LAN-emuleringstesterna.

Brandväggsutvärderarna ger dock såväl ett bu som ett bä. De rycker på axlarna och säger: "som man kunde vänta sig." De har testat åtta brandväggar på två arbetsveckor, och menar att på den tiden får man ett begränsat resultat.

– Vi har haft källkoden bredvid oss men lite tid; för hackers gäller det omvända, säger Robert Malmgren från Incolumitas.

Deras slutsats är att brandväggarna gör ungefär det de ska – med några uppenbara brister, såsom att de alla gått att klippa av. Konsekvensen när brandväggen lägger av är att hela kontakten utåt blockeras. När det hänt några gånger tröttnar kanske företagen och dumpar sin vägg.

De vill gärna betona att brandväggar inte löser säkerhetsproblemen ens om de är uppe.

Med Internet som det är – med t ex Java som en enda stor missbruksmöjlighet – försvinner inte problemen bara med en brandvägg.

Lösningen heter medvetenhet om brandväggars begränsningar och tillgång till utbildad personal. De små företagen kanske inte kan tillhandahålla detta och därför är det viktigt att något görs centralt. Något sådant organ finns ännu inte, men Malmgren och Hagnell säger en förening är i bildande redan i dagarna. □

Svårt med Internet i två moln

Testerna på årets Interopmässa sker inom tre kategorier. Produkttesterna var först ut, i slutet av april skulle resultaten vara inlämnade till Snus (vilket bara delvis uppfylldes). Nätets inre funktioner testas för fullt. Bakom dessa tester på nätfunktioner sitter Snus Nätoperativcentral, NOC, tillsammans med operatörerna och undersöker nätets grundläggande funktioner: routingen.

Mässnätet består av tre operatörer, Tele2, Global One (France Telecom) och Telia. De har förbindelse med varandra och NOC via en MIX, Mäss-Internet Exchange.

Operatörerna har sedan kontakt ut mot korskopplingen DGIX, Distributed Global Internet Exchange, vilken i sin tur sköter förbindelsen ut mot resten av världen. Alla företag har en anslutning till en av operatörerna, förutom Cisco och Network Management vilka har anslutning till två operatörer, en sk multihoming. Det gör att paket från dessa företags nätmoln (Autonoma System) kan ta två vägar ut i världen (och sinsemellan).

Detta "multihomade" arrangemang medför ett antal komplikationer. Med hjälp av NOCs Patrik Fältström tränger jag in i den osynliga routingens värld.

NOC har identifierat tre problem, mer eller mindre kända i förväg, som uppenbarat sig.

Protokollet som hanterar routingen mellan olika nätmoln – BGP4 – har ingen lastbalansering. Belastningen väljer en väg fram till målet även om flera finns tillgängliga. Bara när den ordinarie vägen är ur funktion väljs nästa. Prestandan blir därför lidande.

Assymetriproblemet har varit till stort besvär. Av debiteringsskäl vill varje nätmoln att en inkommande linje ska gå kortaste väg internt, det vill säga att en utgående linje inte kommer in i en del av nätet fysiskt långt från slutmålet så att internkostnaderna blir stora (ISDN-belastningar och annat).



Patrik Fältström ur NOC-gruppen reder ut routingbegreppen.

Om en användare under Telias AS vill prata med ena hörnet av KTH-molnet, är det inte bra (för KTH) om Telia direkt routar över paketet till ett diametralt motsatt hörn i KTH-nätet. Därför sätter man på ett filter som förvägrar en sådan förbindelse tillträde, och ser till att varje paket går längsta möjliga väg på "eget" territorium. Har Telia en anslutning närmare målet in mot KTH-molnet, väljs denna istället.

Detta leder till en asymmetri, eftersom en förbindelse kommer att routas olika åt olika håll. Därför sätter man ut filter dels inom molnen och gentemot andra moln, vilket ska stoppa denna asymmetri.

Det sista problemet är mer en logisk kullerbytta än ett egentligt problem. Med mulithoming kommer ett företag som har två operatörer att behöva välja sekundäroperatörens adress, dess CIDR-block, istället för primärleverantören. Detta då routrarna specialannonserar subnät (IP-adresser) som avviker från molnets huvudadress (CIDR-block). Subnätet har en längre adress – den är mer specifik – och routern väljer den väg som annonserat den längsta korrekta adressen.

När företagen kör sina tester och demonstrerar sina produkters kvaliteter, slungas datan runt i ledningarna på ett sätt inte ens operatörerna och NOC är medvetna om. Men de närmar sig detta medvetande.

NIKLAS MÖLLER

Cisco blev ett spöke i nätet

Routingjätten Cisco hade inga tekniska problem med att ansluta sig som Autonomt System mot både Global One och Tele2, enligt Ciscos Niklas Montin. På första mässdagens morgon hade de sina fysiska förbindelser uppe och allt fungerade – förutom att de var osynliga för yttervärlden.

För att en router ska acceptera väginformation av en annan router, kräver den en manuell inrapportering av sin egen administratör. Det räcker inte att det illvilliga företaget TeliasKonkurrent anmäler att man kan nå Telia via deras AS för att en vägledande router ska låta paket komma den vägen – för att sedan hamna i papperskorgen. Vägen måste annonseras och manuellt godkännas.

Mässans nätadministratörer hade inte i tid anmält detta till de externa nätmolnen.

Därför spelade det föga roll hur mycket Ciscos unika AS annonserades via Tele2 och Global One, ingen router brydde sig om deras rop.

Cisoc tänker dock pröva med att köra det interna protokollet IGP mot båda operatörerna istället för BGP4, och låtsas vara interna användare. I nuläget har Ciscos mässföretag praktiskt sett endast en förbindelse med yttervärlden.

Redaktör: Niklas Möller, 08 796 66 95, Internet: niklas.moller@datateknik.et.se

Mässnätet på Interop

Mässnätet byggdes på principer som ska kunna skalas upp till Sveriges framtida Internet. Istället för att som nu leda all nationell trafik genom en enda korskopplingspunkt, byggs flera upp. Internationell och nationell trafik kan gå via olika korskopplingar, vilket möjliggör ett snabbare och flexiblare system.

GRAFIK: PER THORNÉUS

I principbilden av mässnätet sitter företagen på varsitt moln. Varje nätmoln representerar ett så kallat AS, Autonomt System. Företag som ansluter sig till endast en annan operatör kan ingå under dennes nätmoln, liksom dem som placerats på de tre större operatörernas moln. Större företag kan ansluta till flera olika nätmoln, men måste då bilda ett eget moln. De mindre molnen i figuren är två sådana företag.

Nätmolnen kopplas ihop i korskopplingar, Internet Exchanges (IX), där ett stort antal moln kan nås.

Med tusentals nätmoln sammanbundna i ett jättelikt nätverk är vägvalssystemet, routingen, av stor vikt. För att ett informationspaket ska veta hur det ska nå sitt mål, angivet med en IP-adress, måste nätmolnen tala om vilka moln de i sin tur har kontakt med. I mässexemplet ska Tele2 liksom Global One tala om för alla som är anslutna till MIX och DGIX att bakom dem sitter Ciscos nätmoln.

Om hela "bakomliggande" systemen skulle rapporteras av varje nätmoln som i sin tur för informationen vidare skulle routingtabellerna vid varje moln bli närmast oändliga. Dessutom skulle cirkelrapportering snart bli fallet, där Global One skulle rapporteras tillgängligt såväl direkt från DGIX som via Tele2 och Cisco.

För att stävja dessa avarter av informationsrapportering finns regleringar i protokollen som hanterar routingen mellan nätmoln. Ett nätmoln i Japan behöver inte hålla reda på den exakta lokaliseringen av en svensk organisations adress. Istället finns ett system som i princip ämnar fungera som när man skickar brev. Istället för att med namn, postadress, postnummer och land för varenda adress, räcker det utanför landet att signalera "Här finns Sverige", och så sänder alla huvudpostkontor sina paket som avslutas med "Sverige" till just oss. För Internetadresser fungerar det analogt, även om den geografiska indelningen inte är lika strikt.

En naturlig konsekvens av att endast begynnelseblocken av en Internetadress (IP-adress) behöver stämma för att ett paket ska kunna skickas åt det hållet, är att routern väljer den mottagare som annonserar längsta överensstämmelsen med sökt adress.

Ett problem med anslutning till två operatörer blir då – med mässnätet som exempel – att Cisco blir tvungen att välja en IP-adress med sekundärleverantörens Global Ones prefix istället för huvudleverantören Tele2, om förbindelsen ska gå via Tele2's nätmoln. Routrarna specialannonserar nämligen ut de adresser som avviker från huvudprefixen. Om Cisco skulle välja en typisk Tele2-nummersvit, skulle Telia utåt inte adressera just de adresserna, medan Global One skulle anonnsera hela adresserna och därmed "få" paketen.

Om en ledning bryts vidarebefordrar routrarna informationen genom hela systemet så att det elektroniska paketet kan ta en annan väg än via den ledningen. Det mesta sker automatiskt, endast tillåtna vägar och accepterade AS definieras manuellt. Detta för att undvika missbruk där nätmoln kan annonsera tillgång till en adress den egentligen inte alls har förbindelse med.

NIKLAS MÖLLER

ta protokollet.

Vad vore dock övningar utan det väntat oväntade? Trots den stora automatiseringen i Internet sköts vissa funktioner manuellt. En sådan är inmatningen av accepterade nätmoln. Två av mässföretagen hade väl fungerade förbindelser till två operatörer. Men ingen i det utomstående nätet kunde nå dem, då deras nätmoln inte fanns inskrivna i omvärldens routrar. Snusoperatörerna hade inte i tid anmält dem. Så trots att Telia, Tele2 och Global One sa till sin omvärld att "här finns två splitternya moln", så var det ingen router utanför mässan som trodde dem.

Interoperabilitet står för samarbete, samarbete inom öppna system, och är det något årets mässa visat så är det vikten av samarbete mellan operatörerna. I Sverige är samarbetet gott vad gäller routing och korskopplingar, säger Patrik Fältström. Australien är ett exempel på motsatsen: de har inte en enda korskoppling, utan trafiken mellan landets operatörer går via USA.

NIKLAS MÖLLER

Enklare e-post med gemensam standard

AV ANDERS WALLERIUS

Nu ska det bli enklare att skicka e-post mellan olika elektroniska postsystem.

De största, svenska e-postoperatörerna har kommit överens om gemensamma principer för adressering. Därmed finns grundförutsättningen för att e-post ska kunna skickas från ett postsystem till ett annat

Idag har de olika operatörerna egna adresser för sina kunder. Någon gemensam standard har inte funnits och Internet-post har inte kunnat skickas säkert från operatörer som använder Internet till de som använder X.400, och vice versa. Situationen motsvarar den som gällde för telefonin på 1920-talet.

Men i framtiden ska varje användares e-postadress vara unik, oberoende av operatör, och registreras i ett nationellt register. Operatörens namn ska inte vara en del av adressen, som nu i X.400. Adressen ska också kunna flyttas med om användaren byter operatör.

Överenskommelsen gäller bara i Sverige. Och det kommer att dröja flera år innan posthanteringen mellan operatörerna fungerar automatiskt. ❑

Enighet om datorpostadresser

Datorpostoperatörerna i Sverige har kommit överens att införa gemensamma adresser för Internetpost och X.400-post inom landet. En adress som registreras i det ena systemet ska automatiskt också registreras i det andra.

Med en sådan regel blir det enklare att utbyta datorpost mellan de två världarna genom att adresser kan översättas automatiskt.

– Kärnan i vårt förslag är att varje organisation ska kunna få ett "datorpostnamn" som är unikt i bägge systemen, säger Östen Frånberg, ordförande i nätanvändarföreningen Snus och en av de pådrivande bakom överenskommelsen.

Datorpostnamnet, som närmast motsvarar en domänadress i Internetpost eller en PRMD i X.400, ska tillsammans med landskoden SE utgöra en tillräcklig adress, enligt de nya reglerna. Det innebär att X.400-operatörerna har fått ge med sig i den stora knäckfrågan, om operatörsnamnet ska ingå i adressen eller ej. Det finns där i X.400, det saknas i Internetpost och det kommer alltså inte att ingå i de gemensamma adresserna.

Operatörerna är också överens om att datorpostnamnet tillhör organisationen som använder det. Om man byter operatör ska man alltså få ta med sig sitt postnamn. Skulle två organisationer göra anspråk på samma datorpostnamn ska tvisten lösas i en civilprocess.

– I princip kan det förstås bli problem för oss med speciella regler för Sverige, eftersom vi har kunder i flera länder. Men i praktiken har vi inte råkat ut för något sådant fall hittills, säger Marie Ahlgren från Unisource, en av de X.400-operatörer som står bakom överenskommelsen.

Hur det nya systemet ska implementeras är en fråga som ska utredas vidare av en arbetsgrupp inom ITS, Informationstekniska Standardiseringen. Gruppen leds av Patrik Fältström från Snus.

LENNART PETTERSSON

Samtrafik mellan mail-system

■ Användningen av elektronisk post växer fort. Ericsson är ett av föregångsföretagen vad gäller användning av elektronisk post, som är dominerande vid kontakter mellan de olika enheterna i Sverige och hela världen.

Vid en presskonferens i mitten av januari presenterade Östen Frånberg ordförande i Swedish Network Users Society (SNUS) i samarbete med Johan Särnqvist på Post & Telestyrelsen (PTS), Bo Viklund på Informationstekniska standardiseringen (ITS) och ett flertal av de största i Sverige verksamma mailoperatörerna en överenskommelse som kan komma att göra livet lättare för e-mailanvändarna till en början inom Sverige.

Utvecklingen i Sverige går så fort att systemen inte alltid hänger med i svängarna, vilket får till följd att meddelanden inte kan nå mottageren. I Sverige finns ett tiotal stora e-mailoperatörer som arbetar var och en för sig på en helt avreglerad marknad.

Problemet för många användare är att man inte kan nå en annan användare som inte finns i samma e-postsystem som det man själv utnyttjar.

Det är ännu för tidigt att kunna koppla sig kors och tvärs genom näten men man är en bra bit på väg nu när ovannämnda organisationer kommit överens om något som man på telefonispråk kan kalla gemensam nummerplan, vilket innebär övergripande principer för adressering och "nåbarhet" inom Sverige. Enkelt uttryckt kan man säga att en användare i ett e-postsystem behåller sin e-mailadress om han också blir användare av ett eller flera andra system.

Vårt företag Ericsson kommer alltså att heta "ericsson" i alla mailsystem och en eventuell plåtslagare Karl Ericsson i Knäckebrödhult kan aldrig komma in och få mailadressen "ericsson".

Lite mer tekniskt kan man säga att det handlar om adress-portabilitet, nåbarhet och adresstransparens för elektronisk post inom RFC822- och X.400-standarder i Sverige.

Det tekniska arbetet i den nybildade arbetsgruppen som får ansvaret för de nationella e-postfrågorna i Sverige. Den leds av SNUS med en representant från varje e-mailoperatör.

BENGT SAND



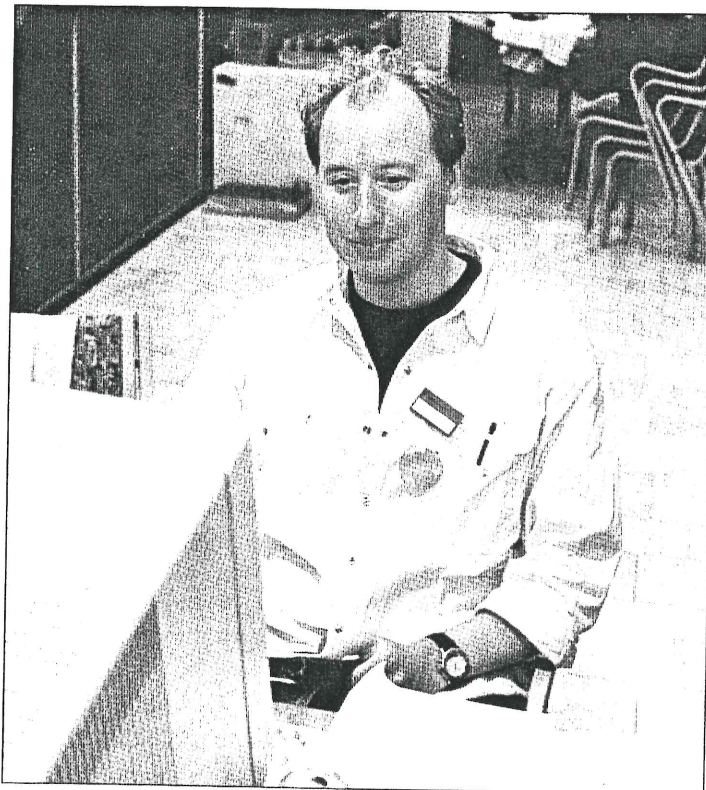
Östen Frånberg (närmast kameran), ordförande i SNUS och till vardags datastrateg på Ericsson Utvecklings AB tillsammans med fr v Bo Viklund, Informationstekniska standardiseringen och Johan Särnqvist, Post & Telestyrelsen.

Foto: BENGT SAND, EUA

Nya grepp på Interoperabilitet -96:

SNUS bygger realistiskt nätlandskap direkt på mässgolvet

Nätanvändarföreningen SNUS satsar på ett helt nytt grepp när nätkonferensen Interoperabilitet –96 slår upp portarna på Sollentunamässan den 8–9 maj. I år bygger man upp ett Sverige i miniatyr - direkt på mässgolvet. Realism är honnörsordet i årets tester, och till seminarierna har en rad utländska talare bjudits in.



Niklas Gerdin har hand om LAN-emuleringstesterna under årets Interoperabilitet -96 på Sollentunamässan.

Det är intressant att följa hur föreningen SNUS förändrar och förbättrar sina årliga nätkonferenser. För bara några år sedan rymdes alltihop i Electrum i Kista. Därefter flyttades arrangemangen till en betydligt större lokal i Folkets hus, mitt i Stockholm. Men efter förra årets interoperabilitet var det åtskilliga medlemmar och yttre intressenter som uttryckte kraftigt negativa åsikter om både program och lokaliteter. SNUS-ledningen tog naturligtvis åt sig kritiken, och i år är följdaktligen både formen och platsen helt ny. Onsdagen den 8 maj invigs Interoperabilitet -96 på Sollentunamässan norr om Stockholm med en stor och öppen utställningsyta som kommer att användas till en helt ny typ av test- och demonstrationsverksamhet.

Mini-Sverige

Nätkonferensen koncentreras i år kring något som kallas "IT-Country". Det hela handlar om att bygga upp ett slags nät-Sverige i miniatyrformat. Ett nät med realistiska drag där skilda typer av företag ansluts till flera olika publika datanät. Utmaningen i sammanhanget är att få utrustningen att fungera ihop med nätet som det anluts till, och att få trafiken att flöda smärtfritt mellan godtyckliga punkter i de olika publika näten.

Näten kommer i princip att bebos av tre skilda typer av företag som är tänkta att representera de olika svenska företag som ansluts till Internet idag.

Den minsta företagstypen utgörs av småföretag som ansluts till en publik IP-tjänst där nätoperatören placerar ut en router för att hantera trafiken. Det något större företaget äger sin egen router och driver egna tjänster, till exempel en domänserver (DNS). Företaget är dock fortfarande anslutet till en enda nätoperatör. Det sker via en brandvägg med en så kallad skyddad zon och en eller flera barriärdatorer (bastion hosts).

Det kommer också att finnas stora företag uppkopplade mot näten i IT-Country. Sådana företag kommer att kunna ha verksamhet på flera platser i nätet. De använder en eller flera egna routrar och anslutning till flera olika nätoperatšrer. Med andra ord ganska komplexa organisationer.

Eventuellt kommer man också att bygga upp företagsnät där IP-trafiken kompletterats med Frame Relay och ATM.

Tydligare tester

I år försöker SNUS kort sagt skapa tester som är mer allmänt tillgängliga för det tusental antal besökare som väntas till Interoperabilitet -96. Tidigare år har många besökare haft synpunkter på att testerna varit svåra att överblicka och studera i detalj. Förutom IT-Country kommer det naturligtvis också att ske mer detaljerade tester i anknytning till konferensen. Men i stället för att trycka ihop allt arbete till dygnen kring själva konferensen så sker nu en stor del av testerna i förväg – hos de olika leverantšrerna och nätoperatörerna. Konkurrerande företag deltar på sätt och vis i ett slags stort grupparbete där det gäller att koppla ihop sina utrustningar med varandra och protokollföra resultaten. Naturligtvis inför de granskande ögonen hos de testledare som SNUS utsett.

LAN-emulering

Ett av de tveklöst mest intressanta testmomenten i årets Interoperabilitet är LAN-emulering i ATM. Det tidigare ganska diffusa standardläget har nu stabiliserats. I år kommer resultaten troligen att bli mer uppmuntrande än vid tidigare testmšten., då man huvudsakligen lyckades att etablera fysisk kontakt mellan utrustningar av olika fabrikat. Telia, AU-system, Bay Networks, Sun Microsystems, Cisco Systems, UB Networks och 3Com deltar LAN-emuleringen.

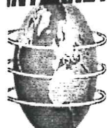
SVANTE NYGREN

Framtidens routing fungerar

Under tre dagar i början av maj visades framtidens Internet på Sollentunamässan. Det var Interoperabilitet -96, en mässa som anordnades av nätverksföreningen Snus, Swedish Network Users Society. På en överblickbar yta hade Sveriges tre största kommersiella Internetoperatörer tillsammans med ett tjugofemtal företag byggt en modell av en framtida Internetuppbyggnad, helt och hållet med dagens teknik.



– *I Sverige är samarbetet gott, säger framtidsingenjören Patrik Fältström från Snus driftcentral. Men dubbla operatörsanslutningar från olika leverantörer kan inte rekommenderas trots detta.*



Modellnätet var uppkopplat via Internet och utgjorde ett praktiskt test av teorier för Internetuppbyggnad i Sverige. Med mässnätet kunde tester i flera plan genomföras.

På en högre nivå testades produkter för brandväggar, lokalnätsemulering och posthantering. På en grundläggande nivå testades själva nätstrukturen. Med större delen av Sverige Internetkunnande på plats kunde principer för en framtida Internetstruktur praktiskt kontrolleras. Slutsatsen: det fungerar! Till största delen, bör tilläggas.

Principerna för mässnätet var uttänkta i förväg, och teorierna för kommunikationshanteringen kände man till. Men det är trots allt stor skillnad mellan teori och praktik. På ett schema ser uppkopplingen så enkel ut, med ringar som symboliserar det ena eller det andra elegant sammanknutet med rena linjer. Men verkligheten är en annan, vilket inte minst syntes på själva mässhallens virrvarr av kablar som vid denna funktionsinriktade mässa inte täcktes av dyra montrar utan var helt synliga.

– Utåt sett gör man inte så många teoretiska upptäckter i en sån här övning, säger Patrik Fältström från Snus driftcentral. Men företag av olika slag och storlek får tillsammans brottas med problemen och det mynnar i en stor förståelse för systemen hos alla som är med.

Den stora frågan om man skulle få ihop systemet kunde ganska snart besvaras med ett ja. Fysiskt sett fungerade förbindelserna på ett tidigt stadium. Men att sedan slussa de elektroniska paketen rätt visade sig bereda problem. Det mesta rådde man till slut bot på, och slutsatsen var tillfredsställande. Strukturen fungerade. "Framtidens Internet idag", som parollen löd, visade sig praktiskt genomförbar.

Modellnätet testade en struktur där de stora operatörerna var kopplade till flera korskopplingspunkter. Detta för att göra systemet snabbt och robust genom att motverka bildandet av flaskhalsar. Idag har Sverige en korskopplingspunkt, DGIX, som fysiskt sitter vid KTH. Mässnätet hade två, den stora DGIX och mässans MIX ("Mäss" Internet Exchange).

För att få en större driftsäkerhet kan större företag och organisationer på analogt vis vara intresserade av att ha fysiska anslutningar till olika operatörer. I mässnätet var två företag, Cisco och Network Management, anslutna till två operatörer.

Routingproblemen var av två slag. Dels av protokollnatur, dels av filtreringsnatur.

Varje Internetanvändare som har fler än en Internetoperatör måste bilda ett eget Autonomt System, ett självständigt nätmoln som använder externa protokoll för att utbyta information med förbundna nätmoln. Protokollet kallas BGP4 och är en Internetstandard. Det fina med BGP4 är att alla använder det, men protokollet har också egenskaper som är mindre lyckade.

Det första problemet med protokollet är att det inte har någon lastbalansering. Varje paket väljer varje gång den väg som definierats som primärvägen, vare sig det finns en bra sekundäranslutning eller inte.

I mässexemplet innebär det att en av de dubbelanslutna företagens ledningar alltid var outnyttjad fast de fysiskt hade dubbla uppkopplingar. Den andra linjen skulle kunna användas till att öka överföringskapaciteten, men blev nu reducerad till endast en backupfunktion. Endast om huvudoperatörens förbindelser gick ner skulle sekundäruppkopplingen komma att användas.

Det andra protokollproblemet är att ett dubbelanslutet företag måste välja sin adress bland de adressblock (prefix) sekundärleverantören har till sitt förfogande, för att förbindelsen ska gå via huvudleverantören. Det är både ologiskt och krångligt, men en följd av vägvalsprinciperna.

Av dessa anledningar rekommenderar Patrik Fältström inte dubbla operatörsanlutningar. Vill ett företag fysiskt ha dubbla förbindelser bör det realisera detta med samma leverantör istället, begära att exempelvis få en förbindelse via Göteborg och en via Stockholm. Då kan företaget få både lastbalansering och backupfunktion.

Det sista problemet kallas asymmetrisk routing, och är något man lätt får om inte vägvalen regleras tillräckligt väl. Asymmetrisk routing kommer sig av att det ur en operatörs synvinkel är klokt att lämna av ett paket så snabbt som möjligt, eftersom all trafik inom det egna nätmolnet bekostas av operatören själv. Om två operatörer resonerar likadant kommer paketen mellan dem ibland att ta två olika vägar beroende på vilket håll de går. Denna asymmetri är olycklig ur debiteringssynpunkt och ska undvikas.

Därför filtrerar operatörerna routinginformationen på ett sådant sätt att paketen ska välja samma väg fram som tillbaka. Praktiskt sett är detta något krångligt och det gäller att definiera informationsflödet rätt i routrarna.

Den asymmetriska routingen fick man att fungera, och konsekvenserna av protokollet BGP4 stod också klara. Övningen var lyckad.

– En förklaring till att Sverige i nuläget endast har en korskopplingspunkt är att kompetensen sitter hos KTHs driftcentral, menar Patrik Fältström. Den asymmetriska routinghärvan, till exempel, löstes av Sverigemästaren i routing, Björn Carlsson på KTHs driftcentral. Än så länge vill inte operatörerna ha fler korskopplingar.

– Det vi nu gör är att titta på alternativa routingprotokoll, säger Patrik Fältström några dagar efter mässan. BGP4 är långtifrån det sis-

SEMINARIER

ONSDAG 8 MAJ

09.00 - 09.10 **Inledning** *Östen Frånberg*, ordförande Snus

09.10 - 09.30 Genomgång av programmet samt förutsättningarna för IT-Country

09.30 - 10.00 Special

10.00 - 10.30 **Kaffe och besök i IT-Country**

MANAGEMENT
10.30 - 12.00

The development of Internet
A view of how the Internet is growing in Asia, and especially what problems people have to get around to get connectivity.
David Conrad, AP-NIC, Tokyo

TEKNIK

Firewalls
Design av brandväggar. Brandväggens plats i helheten

- Andra vägar in
- Kontinuerligt arbete med kontroll av loggar, uppdateringar, omkonfigurationer, dokumenterade förändringar etc.
- Vad skiljer olika firewalls?

Ordförande: *Staffan Hagnell*, Network Management. Med gästtalare.

12.00 - 13.00 **Lunch i IT-Country**

13.00 - 14.30

World Wide Web
Vilken WWW-teknik ska man använda?
HTML 3.0, HTTP 1.1, Javascript.
Assar Westerlund, KTH.
Med gästtalare.

Tester av firewalls?

- Vad skiljer olika firewalls?
- Hur kontrollera säkerheten?
- Vilka testverktyg finns?
- Vilka olika testmetoder finns?

Ordförande: *Staffan Hagnell*, Network Management. Med gästtalare.

14.30 - 15.00 **Kaffe i IT-Country**

15.00 - 16.30

Att bygga e-postsystem i Sverige
Samtrafik mellan olika mailvärldar, rekommendationer för operatörer i Sverige, regler för mappning av namn, pågående arbeten inom Informations tekniska Standardiseringen.-
Lars-Johan Liman, KTH Network. Operations Centre.

Publishing large amount of information
A discussion about problems and solutions to problems arising when handling large amount of information for multilingual customers
Dirk-Willem van Gulik , Joint Research Centre of the European Communities, Ispra, Italy

TORSDAG 9 MAJ

SEMINARIER

09.00 - 09.30 Special

09.30 - 10.00 **Kaffe och besök i IT-Country**

MANAGEMENT
10.00 - 12.00

Electronic Cash: The possibilities and their implications

- Account systems versus true electronic money
- Status of ecash related trials and roll-outs
- Protecting the interests of all parties
- Software only, chip cards and hybrid platforms

Inledning: *Rickard Schoultz*, , Sunet
Paul Dinnissen, DigiCash,The Netherlands

TEKNIK

"Finding the closest source"
In the future the Internet will need low-level support for finding the "closest source" for an information object. About recent development in the area, specifically the Sonar system.
Keith Moore, University of Tennessee, Knoxville

12.00 - 13.00 **Lunch i IT-Country**

13.00 - 14.30

ATM- en granskande genomgång

- Möjligheter och begränsningar
- Standardiseringsläge
- Kända problem
- Vilka produkter klarar vad
- Vilka nät har byggts

Ordförande: *Torbjörn Carlsson, Mikael Lundblad*, Network Management.
Med gästtalare.

Multimedia Transport in the Internet
The requirements and solutions for transporting multimedia information over TCP/IP networks and the Internet. Issues of Multicast Protocols, Fair Queuing techniques and Resource Reservation.
Roland Acra, Cisco, France

14.30 - 15.00 **Kaffe i IT-Country**

15.00 - 16.30

Katalogtjänster
Balansen mellan central och distribuerad katalog. Hur hanteras datamängder och aktualitet. X.500 vs Whois++. För och nackdelar X.500/ Whois++ *Patrik Fältström*, Bunyip

Virtual nets
Ordförande: *Östen Frånberg*
Tyrone F. Pike, UB Networks, USA
Lesley Hansen, Cabletron, UK

16.30 - 17.00 Genomgång

Resultatet av integratörernas demonstration i IT-Country

Avslutning Interoperabilitet-96

Med reservation för ändringar



ONSDAGEN DEN 8 MAJ

TEKNIK

"Strukturen av Internet i ett framtida Sverige"
Peter Löthberg Stupi AB

Med en exponentiell ökning av Internet behöver den interna strukturen för såväl logiska som fysiska nät dimensioneras för kanske femtio gånger dagens storlek för att klara de kommande fem åren.

Nationella nät måste struktureras så att de erbjuder en standardiserad gränsyta mellan nättillhandahållare och användare så att generella standardlösningar kan användas samt att byte av operatör kan ske på ett enkelt sätt.

Den Svenska Internetinfrastrukturmodellen siktar på att erbjuda såväl skalbarhet som en sund plattform för öppenhet och konkurrans.

Peter har medverkat i uppbyggnaden av Sunet, Nordunet, Swipnet, Ebone, NSF-ICMnet samt Sprintlink. Förnärvarande arbetar han med höghastighetsnät i USA samt inkoppling av nya länder i Syd-, och Latinamerika till Internet.

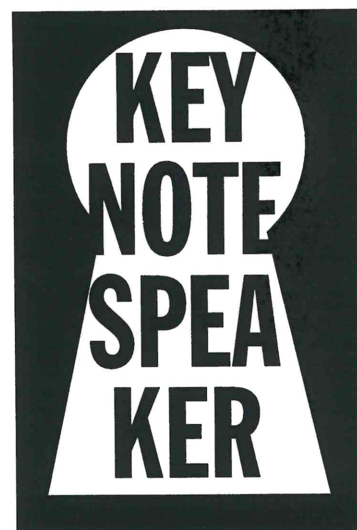
MANAGEMENT

"Trender som ställer krav på kommunikation inom multinationella koncerner"
Johan Särnquist, direktör, AB Electrolux

Av affärsmässiga skäl pågår en utveckling av att centralisera vitala verksamhetsgrenar inom en koncern. Detta medför även stora förändringar inom IT-området som direkt påverkar kommunikationslösningarna. Ett koncernnät kommer att bli en vital komponent för att upprätthålla en fungerande infrastruktur inom en koncern.

Johan har arbetat med kommunikationsfrågor sedan 70-talet, och kommer senast från Post & telestyrelsen där han ansvarat för den "tekniska regleringen inom kommunikationsområdet".

TORSDAGEN DEN 9 MAJ



TEKNIK

Introduction to SNMPv2
David Partain, Managing Director, SNMP Research Europe

What is SNMP2, Progress in standards work, Idéas on transition to SNMP2. The advent of Version 2 of the Simple Network Management Protocol (SNMPv2) provides significant improvements for today´s managers of systems, applications and networks. This presentation will introduce the key enhancements included in SNMPv2, its current standardization status and transition strategies from SNMPv1 to SNMPv2.

SNMP Research, provides leading vendor-independent reference implementations of SNMP-based products.

Reflektioner om ATMs användbarhet idag – marknadsföringen i förhållande till "verkligheten".
Anders Hillbo, KTH, NADA, Systemgruppen, berättar kort om några insikter KTH, NADA fått om ATM bl a inom ramen för de tester vi gjort som deltagare i COAST-projektet (SUNET och TELIA ATM-test) och SGN (Stockholm Gigabit Network).

MANAGMENT

Regeringens IT-proposition, IT-kommissionen och toppledarforum
Ann-Marie Nilsson STATTEL-delegationen

Myndigheter samt industrins engagemang i arbetet med att ta fram IT-propositionen. Vilken betydelse har IT- propositionen för företag, myndigheter, utbildning och allmänhet? Får vi ändrade spelregler? Vilka frågor behöver belysas ytterligare, tex arkitekturen för framtida datanät i Sverige. Arbetet i toppledarforum, pragmatisk modell för att genomföra beslut.

SNUS - Swedish Network Users Society

SNUS är en nätverksförening i Sverige som har som mål att:

- Öka förståelsen för nätverksteknik och -byggande inom såväl användar- som leverantörsleden.
- Driva på utvecklingen vad gäller samtrafik och samverkan mellan operatörerna.
- Testa vilka produkter och system som fungerar i verkligheten.
- Sprida kunskap och erfarenheter genom seminarier, demonstrationer och testrapporter.

SNUS medlemmar återfinns i mer än hundra svenska företag, även privatpersoner är välkomna som medlemmar. Bland medlemsföretagen återfinns såväl storföretagen som små kunskapsföretag. Styrelsen består av personer från såväl storföretag som högteknologiska spjutspetsföretag och forskningsvärlden. Alla delar ett intresse av att föra utvecklingen framåt.

Under SNUS korta historia har vi bl.a. initierat Swipnet (det första kommersiella IP-nätet i Sverige) och medverkat till en överenskommelse om samtrafik för elektronisk post (mellan X.400- och Internet-världarna). SNUS genomför också årligen flera medlemsmöten med seminarier där intressanta ämnen tas upp.

Bli medlem i SNUS och var med och påverka framtiden!
För mer information kontakta vårt kansli på telefon 08-665 60 53
eller via e-mail <snus@snus.se> eller besök vår hemsida; http://www.snus.se/SNUS/

MEDLEMSSKAP

Som medlem i SNUS får du:

- fortlöpande information om SNUS verksamhet.
- förmånligt pris för deltagande på SNUS seminarier
- rösträtt på SNUS årsmöte
- rätt att delta i SNUS arbetsgrupper
- tillgång till forum där du kan tillföra och utbyta erfarenheter

MEDLEMSAVGIFT

Personligt privat medlemsskap (P) 250:-

Företagsmedlemsskap

1-10 st anställda	(F1) 1 000:-	1 kontaktperson
11-100 anställda	(F2) 2 000:-	2 kontaktpersoner
101 & fler anställda	(F3) 3 000:-	3 kontaktpersoner

Kontakta SNUS kansli för medlemsansökan.
Medlemsansökan godkänns av SNUS styrelse och medlemsavgiften faktureras.

SNUS, Box 396, 101 27 STOCKHOLM
tel 08-665 60 53, fax 08-665 80 48 ,
<snus@snus.se> http://www.snus.se/SNUS/

